SERBIAN ASSOCIATION
FOR CRIMINAL LAW
THEORY AND PRACTICE

INSTITUTE OF
CRIMINOLOGICAL AND
SOCIOLOGICAL RESEARCH

JOURNAL
OF CRIMINOLOGY AND CRIMINAL LAW

REVIJA ZA KRIMINOLOGIJU I KRIVIČNO PRAVO

UDK
343

VOL 61
No 1

BELGRADE, 2023

JANUARY – MAY 2023

SERBIAN ASSOCIATION
CRIMINAL LAW THEORY AND PRACTICE

INSTITUTE OF CRIMINOLOGICAL
AND SOCIOLOGICAL RESEARCH

JOURNAL
OF CRIMINOLOGY AND CRIMINAL LAW

REVIJA ZA KRIMINOLOGIJU I KRIVIČNO PRAVO

BELGRADE, 2023

ISSN 1820-2969 (Štampano izd.)
ISSN 2956-2198 (Online)

The Journal is issued by: Serbian Association for Criminal Law Theory and Practice,
Kraljice Natalije 45, sukp@sezampro.rs, +381 11 26 58 019 and
Institute of Criminological and Sociological Research in Belgrade,
Gračanička 18, krinstitut@gmail.com, +381 11 2625-424.

The Journal is published three times a year. The Journal is indexed in HeinOnline and Crossref

All articles and papers should be sent via online platform at https://rkkp.org.rs/

Supported by the Ministry of Education, Science and Technological Development

Printed and arranged by: "Službeni Glasnik", Belgrade. Number of prints: 300

Subcription for individuals is 3,000 RSD, and for legal entities 10,000 RSD

JOURNAL
OF CRIMINOLOGY AND CRIMINAL LAW

VOL 61 No. 1 BELGRADE JANUARY – MAY 2023

UDK 343 ISSN 1820-2969

C O N T E N T S

ARTICLES:

Academician Miodrag SIMOVIĆ*
Vice-president, Constitutional Court of BiH
Full professor of the Law Faculty
at the University of Bihać

Full member of Academy of Sciences
and Arts of Bosnia and Herzegovina

Mile ŠIKMAN, PhD**
Associate professor at the
Law Faculty in Banja Luka

Original Scientific Article
Received: 19 May 2022
Accepted: 28 February 2023
UDK:343.988-053.2/.6:004.738.5
159.922.72
https://doi.org/10.47152/rkkp.61.1.1

THE IMPACT OF DIGITAL ENVIRONMENT ON CHILDREN AND RESPOND TO SOCIALLY UNACCEPTABLE BEHAVIOR

The influence of digital environment on the psychophysical development of children is becoming more and more dominant, which is supported by empirical indicators. The type and degree of influence can be different, and the consequence is always the same and is reflected in the harmful effects on the psychophysical development of children. At the same time, numerous studies on victims show that the real impact of high technology on the psychophysical development of children is much greater than that shown by the available data. The main reason for such a situation could be sought in the reasons for non-reporting of these behaviors by the victim or rather non-recognition of the harmful effects of high technology on the psychophysical development of children. To this, we can add the detrimental effects of secondary victimization, which often covers victims of crime. In this sense, the question arises as to how society can most adequately respond to these behaviors. Different

* e-mail: vlado_s@blic.net
** e-mail: mile.sikman@pf.unibl.org

models of prevention can yield promising results, but raise questions about protection of children's rights, including personal data. On the other hand, criminal repression, as ultima ratio, has full justification for its introduction, but also significant limitations. This is why the subject matter of this paper is prevention and suppression of socially unacceptable behavior manifested by the use of high technology, regardless of whether children are victims or actors of such behavior.

Keywords: digital environment, children, criminal offense, general prevention, special prevention

1. Introduction

As we are witnessing that the development of modern technologies has greatly affected people's daily lives, we are aware that its use has changed all spheres of human activities and life. That is why today we are talking about a "digital environment" that encompasses information and communication technologies (ICT), including Internet, mobile and related technologies and devices, as well as digital networks, databases, contents and services (Council of Europe, 2018). It seems that this trend is growing rapidly in the times ahead, and will be reflected in the mass use of transformative technologies in every activity of modern life[1]. This thesis has already been confirmed during the Corona virus pandemic (since 2020), which has affected even greater exposure of children to high technologies, both due to obligations (distance learning) and due to measures introduced during the pandemic (restriction of movement)[2]. Thus, the digital age has created a new kind of reality, the so-called „digital reality“, which brings new challenges for both the individual and society (Pylkin, Serkova, Petrov & Pylkina, 2021), which directly affects the psychophysical development of children, their communication and behavior[3].

1 For example, Israeli publicist Yuval Noah Harari in his novel Homo Deus - A Brief History of Tomorrow (2015) visionarily states: „Cyber-engineering shall go one step further, merging organic body with inorganic devices such as bionic fists, artificial eyes or millions of nanorobots that will move through our bloodstream, diagnose problems and repair damages" (Harari, 2015: 61).

2 Consumption of social media via Internet, according to the Global Web Index, increased significantly in all age groups during the Coronary virus pandemic, with a significant difference in the content they used. So the so-called Generation Z (ages eight to 23) spent most of their time listening to music (53%) and playing games (45%), emphasizing their interest in entertainment content (GlobalWebIndex, 2020).

3 It was the research conducted by UNICEF under title "The State of the World's Children" in 2017 that confirmed the thesis that digital technologies have affected all spheres of children's social life (UNICEF, 2017).

Starting from the fact that the psychophysical development of children is not static and fixed, and is continuously exposed to changes, it is quite realistic to expect changes associated with high and transformative technologies. Many of them have already manifested themselves, and some are going to be the subject of manipulation and abuse. So, the fact is that with the appearance of new technologies, their abuse for anti(social) purposes is present, including criminal ones, so that almost all forms of negative behavior, as well as crimes known in real life, can be committed in virtual world. Thus, children are very often victims of crimes on the Internet. According to findings of Europol, sexual exploitation of children on the Internet includes a range of criminal activities, such as sexual abuse and exploitation of children via Internet[4], production and distribution of pornographic content, *online* inducement of children for sexual exploitation, "live" abuse of children at a distance, and one particularly worrying trend called "deep lie", which is based on the misuse of *AI based* technique[5] (Europol, 2019, 34). In addition, we can add the problem of manipulation of personal data, given that today they represent one of the greatest values, which are multiply endangered in the digital world (Šikman, 2020).

That is why we have one, we could say, paradoxal situation: modern technologies create new and unimaginable possibilities, but also open new dangers and have consequences for the psychophysical development of children. Namely, changes can be considered in a positive and negative context. The positive context is mentioned in the part of the changes that have led to leaving some manual and routine tasks to automatic devices, which leaves the individual more time to engage in creative activities and greater expression of their own individuality. Also, the use of assistive technology (any item, piece of equipment, software program or product system) enables daily functioning and involvement in activities and significantly contributes to the quality of life of persons with disabilities and children with disabilities (Lancioni, Sigafoos, O'Reilly, & Singh, 2013). Today's generations use all the advantages provided by high technologies for communication[6], grow up with

4 While sexual abuse or exploitation is accessible in the physical world, the subsequent sharing of images and videos significantly exacerbates the impact of these crimes. Namely, the amount of this data on the network is astonishing and continues to increase. As the number of young people and children accessing the Internet increases, so do criminals, who consciously misuse the anonymity and possibilities of the Internet (Europol, 2019: 30).

5 This technique uploads photos or videos over another video. It has already been used to place the faces of celebrities on existing pornographic videos. Although the technology is still relatively new, it is rapidly improving and becoming more accessible and easier to use (Europol, 2019: 34).

6 „The new generation of children is also described as the generation of digital thinkers. Older generations are focused on semantic symbols, while younger generations find meaning in every symbol on the Internet, every icon or link, and turn them into information" (Mićević-Karanović, Mesaroš-Živkov, Pavlov & Brkljač, 2020: 35).

the use of digital devices and consumption of Internet content, certainly including well-known social networks[7] (You Tube, Facebook, Instagram, TikTok and others). Therefore, today, children are growing up using multifunctional technological devices from the earliest childhood. Thanks to them, they have no problem to "keep up with information flows, to cope with information overload, to engage in virtual communication, to communicate and cooperate through the Internet" (Mićević-Karanović, Mesaroš-Živkov, Pavlov & Brkljač, 2020: 36).

At the same time, the influence on their psychophysical development is evident, which certainly reflects on the quality of life and growing up. Namely, deep involvement in digital reality and active application of its technical mediators burden the psychophysics of the individual, which, especially in the phase of rapid growth, not only deforms patterns of behavior, but can affect the formation of brain structures (Pylkin, Serkova, Petrov, & Pylkina, 2021). In fact, the results of 2019 survey found that "almost all young adolescents (95%) had access to the Internet: 67% owned mobile phone and 68% had an account on social networks. Mobile phone ownership was not associated with any indicators of well-being (math and reading test scores, school affiliation, psychological problems, behavioral problems, or physical health) after control of demographic factors. Possession of accounts on social networks and the frequency of use of social media were strongly associated with behavioral problems (explaining ~3% of variations in behavioral problems). Despite the lack of strong associations, 91% of adolescents reported at least one detected technology-related impairment, and 29% of adolescents reported application of negative experiences from Internet to offline" (George, Jensen, Russell, Gassman-Pines, Copeland, Hoyle, Odgers, 2020).

This issue is the subject matter of this paper. How and in what way to accept the reality (and usefulness) of the use of high technologies by children and, at the same time, ensure their protection and safety. Also, it is necessary to pay attention to the limited scope of various prevention mechanisms, above all criminal protection. We emphasize this because the impression is that by prescribing crimes protecting children from the effects of high technology (e.g. certain criminal offenses from the group of crimes of sexual abuse and exploitation of children), this problem is actually solved. Certainly, by prescribing these criminal offenses, the effects of general prevention can be achieved, but we should not lose sight of the fact that these cases are often the so-called irreparable recidivists, who will seek to use high technology to abuse children. In this sense, the focus should be on

7 According to statistics from the Family Survey, children from developed countries spend an average of seven hours and 30 minutes each day in front of some kind of screen, be it television, computer, smartphone (Rideout, Foehr, Roberts, 2010; Pavlović, & Vulić, 2014).

criminal law solutions that can give better results, such as preventive detention (modeled on certain countries).

2. Consequences of the use of high in children

The process of informatization leads to the dehumanization and alienation of individuals, and over time to the loss of their identity (Veljović, Vulović, & Damnjanović, 2009). All this leads to physical inactivity (hypokinesia) and to the loss of stimulus for proper growth and development. The “sitting man” is not physically active and consumes less energy for daily activities, which results in certain physical and psychological problems, and above all leads to obesity, physical deformities, loss of muscle mass, hypertension[8], weakening of density and elasticity of joints and ligaments, weakening of respiratory and cardiovascular capacity, vegetative and psychological disorders (Mićević-Karanović, Mesaroš-Živkov, Pavlov, & Brkljač, 2020: 34). Thus, for example, research suggests that adolescents who spend more time on new media (including social media and electronic devices such as smartphones) are more likely to report mental health problems than adolescents who spend more time activities not including screen (personal social interaction, sports/exercise, homework, consumption of print media and attendance at religious services) (Twenge, Joiner, Rogers, Martin, 2018). However, recent research comes to opposite conclusions, i.e. that no significant correlations can be established between these two variables (Odgers, Jensen, 2020; Orben, 2019), which actually shows mostly low quality of studies on this topic (Orben, 2019).

In fact, the results confronted in this way are not surprising, because it is generally known that a number of social, genetic and experiential factors influences the development of mental illness. Likewise, the virtual world can be confusing for a child, which can cause indistinguishability of reality from imagination (Allington, McGill-Franzen, Camilli, Williams, Graff, Zeig, Zmach, & Nowak, 2010). The experiences that children adopt by using high technology are part of their daily lives. Thus, some research has shown that young people (aged between 21 and 30) feel lonelier than middle-aged and older people do (between 50 and 70 years old) (Degges-White, 2018). In addition, conflicts within families are

8 Research suggests that sitting at a computer for too long has direct consequences on the proper growth and development of children, as well as the incorrect sitting position of children (Straker, Pollock, Burgess-Limerick, Skoss, & Coleman, 2008; Geldhof, Cardon, De Bourdeaudhuij, & De Clercq, 2007; Murphy, Buckle, Stubbs, 2004 cited in: Mićević-Karanović, Mesaroš-Živkov, Pavlov, & Brkljač, 2020: 35).

increasingly linked to the use of technology by children[9]. Unfortunately, many young people, in addition to not experiencing certain social experiences that only *offline* world provides, in childhood were often deprived of meaningful interaction with their parents who themselves were preoccupied with their own digital devices.

A special problem is the dangers to which children are exposed in digital environment. They can be of the same level and degree as the dangers in the real world. Researchers usually divide this wide range of risks encountered on the Internet into three categories: content risks, contact risks and behavioral risks (Miladinović, 2018: 24). Content risks relate to a child's exposure to unwanted and inappropriate content, which may include sexual, pornographic and violent photographs, certain forms of advertising, racist and discriminatory material and violent speech materials, websites promoting unhealthy and dangerous behaviors such as self-harm, suicide or anorexia. Contact risks relate to a child's participation in risky communication, for example with an adult seeking inappropriate contact or a child for sexual purposes, or with individuals seeking to radicalize a child and persuading him or her to engage in unhealthy and dangerous behaviors. Behavioral risks imply child's behavior in a certain way that contributes to the emergence of risky behavior or relationship. This may include children who write negatively about other children or create hateful materials towards other children, encouraging racism or publishing and sharing sexual images, including material they have created themselves (Miladinović, 2018: 24). It is a so-called digital peer violence (cyberbullying).

Furthermore, new technologies, such as cryptocurrency and the dark internet - encourage the direct showing of sexual abuse of children and other harmful content, and pose a challenge to law enforcement (UNICEF, 2017). Data manipulation is misuse of information technology for the purpose of covert influence on another person's decision-making, in a way that exploits his weakness (Susser, Roessler, Nissenbaum, 2019). Online manipulation can be observed through the data collection cycle, profiling of users and finally micro targeting and manipulation (European Data Protection Supervisor, 2018). It seems that the last phase of this cycle significantly endangers numerous rights and freedoms of citizens, and thus enters the criminal zone. And, as stated in the Opinion of the European Data Protection Supervisor (2018), "the problem is real and urgent, and

9 Thus, for example, research has shown that time spent in front of a screen is one of the common causes of conflict between parents and children. Thus, 25% of surveyed families argued about the time spent in front of the screen, while 10% of them clashed over the way children spend their time on the Internet (Livingstone, Blum-Ross, Pavlick, Ólafsson, 2018).

is likely to worsen as more people connect to the Internet, with the increased role of artificial intelligence system" (European Data Protection Supervisor, 2018).

Many of these behaviors are characterized as criminal offenses, while others are an introduction to prohibited behaviors. What could be stated as common is that the consequences of violence on the Internet are felt by everyone: victims, perpetrators and observers (Lalić, 2020).

3. Prevention of the negative impact of digital environment on children

The rights of children in the digital environment have been under discussion for some time. Thus, the United Nations Committee on the Rights of the Child issued a recommendation that all children should have safe access to high technology and digital media, and should be allowed to fully participate, express, seek information and enjoy all the rights contained in the UN Convention on the Rights of the Child and its Optional Protocols, without any discrimination. "It starts from the fact that the digital environment is crucial for the realization of children's rights and that every child has the right to access digital world, as well as to play, learn and progress in that world, while being protected as best as possible". It is in fact the preamble to the Final Statement on the Rights of the Child in the Digital Environment adopted by the European Network of Ombudsperson for Children in 2019 in Belfast (European Network of Ombudsperson for Children, 2019a).

The Council of Europe's position is also set out in the Declaration of the Committee of Ministers on the need to protect the privacy of children in the digital environment from 2021, in accordance with Article 8 of the Convention, which emphasizes the need to respect the child's right to private and family life in digital environment, which includes the right to information self-determination and protection of personal data and communications. As a risk, children's privacy may arise from the design and function of digital technologies and services, as well as children's own activities and those of their parents, peers, educators or others in digital environment; (Council of Europe, 2021). Thus, the commitment to the protection of children's rights to non-discrimination, access to information, freedom of expression and participation in digital environment in cooperation with other participants acting in the digital environment has been unequivocally confirmed.

In that sense, the question arises as to how society can influence the reduction of negative effects of high technologies on the psychophysical development of children. Attention should be drawn to the normative texts adopted by the Committee of Ministers of the Council of Europe, which are designed to help

member states deal with these risks and, as a consequence, to ensure the human rights and fundamental freedoms of children. These texts include Recommendation CM/Rec(2018)7 of the Committee of Ministers to member states on Guidelines for the Respect, Protection and Exercise of the Rights of the Child in the Digital Environment; the new Handbook for Policy Makers on the Rights of the Child in the Digital Environment (2019) which completes these guidelines, supporting policy makers in dealing with rights on the Internet and protecting children; Council of Europe Strategy for the Rights of the Child (2016-2021); Recommendation CM/Rec(2014)6 of the Committee of Ministers to member states on the Guide to the Human Rights of Internet Users; Recommendation CM/Rec(2009)5 on measures to protect children from harmful content and behavior and to promote their active participation in the new information and communication environment; Recommendation CM/Rec(2008)6 on measures to promote respect for freedom of expression and information regarding internet filters; 2008 Declaration on the Protection of the Dignity, Safety and Privacy of Children on the Internet; Recommendation CM/Rec(2007)11 on the promotion of freedom of expression and information in the new information and communication environment; Recommendation CM/Rec(2006)12 on the empowerment of children in the new information and communication environment and Recommendation CM/Rec(2011)8 on self-regulation regarding cyber content (self-regulation and protection of users from illegal or harmful content on new communication and information services). In addition to the above documents, it is worth noting the Recommendation on the Rights of the Child in the Digital Environment, adopted by the European Network of Young Advisers of the Ombudsperson for Children in 2019 (European Network of Ombudsperson for Children, 2019b).

In terms of these documents, prevention should be focused on providing children with the knowledge, skills, understanding, attitudes, values of human rights and behavior necessary for active participation in digital environment, as well as for responsible action while respecting the rights of others. There is also a need to encourage trust and promote trust on the Internet, in particular by neutral labeling of content to enable both children and adults to make their own value judgments about content on the Internet. It is also necessary to strengthen cooperation with private sector actors and civil society, in order to develop and promote coherent strategies to protect children from content and behavior that carry the risk of harm, while advocating for their active participation and best possible use of new information and communication environment.

This encourages the development and use of safe spaces, as well as other tools that facilitate access to child-friendly websites and Internet content, promotion of further development and voluntary use of trust marks and stamps that al-

low parents and children to easily distinguish harmless content from the content that carries the risk of harm, as well as promotion of the development of skills in children, parents and educators for better understanding and facing with contents and behavior that carries the risk of harm. Among many topics covered are protection of personal data, provision of content adapted to children and their developmental capacities, helplines and hotlines, vulnerability and resilience, and the role and responsibilities of business enterprises.

Findings from some studies suggest that prevention messages should be focused on youth behavior rather than certain online sites where socially unacceptable behaviors occur (Kimberly, Finkelhlor, Jones, Wolak, 2010). In addition, some researchers believe that the impact of high technology can be reduced through parental media mediation. “It is important that we understand why we allowed a child to watch certain television content at a certain time, and what the child can learn from it. Parents must focus on positive aspects of modern technology, and take advantage that modern technology provides, not ignoring the negative aspects but finding certain solutions to mitigate the negative impact. In accordance with the age of the children, parents should give child freedom to decide on the use of certain digital devices” (Mataušić, 2002: 451). It is important to understand that prohibition to watch certain content does not help the child’s behavior, i.e. that there is a counter effect because the child then begins to fight with parent and the child develops resistance to parent. Therefore, it is important to establish the time in which the child will be able to have access to some media content. In addition, it is important for parents to be aware that they will be able to reduce the time children use for media content only if the remaining free time is used and filled with some other activities (Mataušić, 2002: 451).

4. Criminal protection of children in digital environment

The increasing availability of child pornography by abuse of high technologies in digital environment has conditioned the reaction of international legal entities, and also the introduction of incriminations at the national level. In this regard, the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography from 2000[10], which

10 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, adopted on 25 May 2000 by resolution A/RES/54/263 at the fifty-fourth session of the General Assembly of the United Nations, “Official Gazette of BiH – International Treaties”, Number 5/2002.

requires member states to take actions to guarantee protection of children from child trafficking, child prostitution and child pornography, is significant.

Then, in 2005, the Council of Europe Convention on High-Tech Crime[11] (the so-called Budapest Convention) was adopted, which is, together with two additional protocols[12], the first international treaty on crimes committed via the Internet and other computer networks, dealing specifically with copyright infringement and computer fraud, child pornography and network security breaches. It establishes a common approach to the computer-related criminal offenses and has the aim to make criminal investigations referring to such offenses more efficient. Its main goal, stated in the preamble, is to implement a common criminal policy aimed at protecting society from high-tech crime, in particular by adopting appropriate legislation and encouraging international cooperation. According to this Convention, any behavior related to child pornography must be established as a criminal offense in the signatory states. Child sexual abuse material is defined in Article 9 as “pornographic material that visually depicts a minor engaging in sexually explicit behavior; a person who appears to be a minor engaged in sexually explicit behavior and realistic images representing a minor in sexually explicit behavior”. In order for the material to be considered as child pornography under Article 9 of the Convention, it is clear that a real child does not have to be included, it is sufficient that the material represents a minor. The rationale for this provision is that even if there is no actual harm done to the child in the material production process, it can be used to encourage or seduce children to participate in such actions.

Subsequently, the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[13] (the so-called Lanzarote Convention) was adopted, containing provisions criminalizing the use of new technologies, especially Internet, for sexual harm or abuse of children. This Convention is the first instrument to identify various forms of sexual abuse of children as criminal offenses, including domestic or family abuse, using force, coercion or threats. The definition of child pornography in Article 20 extends the framework

11 Convention on Cybercrime, European Treaty Series - No. 185

12 The first Additional Protocol to the Convention on High-Tech Crime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, was adopted in 2003, and the second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence was adopted in 2021. See more: Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189); Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence.

13 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

of the Budapest Convention in term of including all forms of material, not just material produced through computer systems. The act of "consciously gaining access to child pornography" is also criminalized. The aim of this provision is to identify those offenders who intentionally access child pornography sites, but without downloading any images of child sexual abuse. Preventive measures listed in this Convention include screening, recruiting and training of people working with children, raising children's awareness of risks and teaching them to protect themselves, as well as measures of monitoring offenders and potential offenders. The Convention also establishes victim support programs, encourages people to report suspected sexual exploitation and abuse, and establishes telephone and Internet helplines for children. It also ensures that certain types of behavior are classified as criminal offenses, such as engaging in sexual activities with a child under legal age and child prostitution and pornography. The Convention also criminalizes the instigation of children for sexual purposes and "sex tourism". The new legal tool also ensures that child victims are protected during court proceedings, for example in terms of their identity and privacy.

In addition, in the context of the criminal protection of children in digital environment, we can cite the 1985 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[14]. This document ensures respect for basic human rights with regard to the processing of personal data. As children are holders of data protection rights under this Convention, special attention must be paid to empowering children to exercise their right to data protection.

Finally, under the European Convention for the Protection of Human Rights and Fundamental Freedoms[15] (ECHR) (ETS No. 5), the European Court of Human Rights has developed case law on human rights on the Internet. Examples of the rights in question in such cases include the right to respect for private and family life (Article 8) and freedom of expression (Article 10). The Court published a fact list summarizing all the leading cases in the field of technology and human rights (European Court of Human Rights, 2022).

The mentioned international legal framework, among other things, was the basis for the introduction of these incriminations in the criminal legislation of the Republika Srpska. Thus, the Criminal Code of the Republika Srpska[16] introduced a special chapter on criminal offenses entitled "Criminal offenses of sexual abuse

14 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

15 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005).

16 „Official Gazette of the Republika Srpska" Nos. 64/2017, 104/2018, 15/2021 and 89/2021.

and exploitation of a child", which also criminalized the acts of Exploitation of Children for Pornography (Article 175), Exploitation of Children for Pornographic Performance (Article 176), Introducing children with pornography (Article 177) and Exploitation of Computer Network or Communication by other technical means for committing criminal offenses of sexual abuse or exploitation of a child (Article 178) (Marković, 2018: 36-39). In addition, Article 123, item 7 stipulates that child as a victim of a criminal offense is a person under the age of 18, which may be considered as an adequate legal solution. Although the mentioned legal framework is adequate, it is not fully harmonized with mentioned international legal documents, which affects the problem of application of prescribed provisions (Stojanović, 2018: 615). Some of them concern the institute of "consciously gaining access to child pornography", the incrimination of which could be disputable from the aspect of basic criminal law principles, while the others are of technical nature.

5. Conclusion

Based on the above brief overview of the impact of digital environment on the psychophysical development of children, at least two conclusions can be drawn. The first is that we should not go in the direction of denying the usefulness of high technologies and their use in the daily lives of children and others, that is, the necessity of creating a safe digital environment. In this sense, it is necessary to put emphasis on determining the ways in which high technologies affect the psychophysical development of children and in relation to how society can act properly. The response of society can move in several directions, which is, in fact, in line with the elements of criminal policy: responding by both formal and informal means of social control. Namely, more and more research results call for parental responsibility when it comes to guiding children when using digital devices, but also for the need to increase awareness of their own habits in this regard. This would certainly be the first instance of social control, which would be followed by the activities of educational, cultural, sports and even other institutions. At this level, it is crucial to find ways in which parents, educators and other subjects of informal social control gain greater awareness of the scope of this problem, and thus improve the response to socially unacceptable behaviors.

The second, more important issue is the reaction of the subjects of formal social control. In this part, we should start from the fact that children, as well as adults, are holders of the right to data protection. This is especially important in the context of the digital environment, in which children provide personal infor-

mation without being aware of it in many cases. This is why it is much easier for them to become victims of crime, including child pornography. In this context, it is necessary to create an adequate response of the subjects of formal social control to this problem. When it comes to criminal justice treatment, which is just one of the ways - the incrimination of criminal offenses of child pornography as positive one should be mentioned as positive. What could be stated as negative is inadequate application of these norms in court practice, which is manifested in specific court decisions.

Finally, what we can particularly emphasize is the need for stronger protection for the victims of these criminal offenses. It can be achieved only through adequate and connected action of mechanisms of formal and informal social control. In this process, relying on one or the other alone is not enough. This is especially applicable on criminal law reaction, which, if the absence of informal reaction is noticeable, does not have much chance of success.

Literature

- Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)
- Allington, R. L., McGill-Franzen, A., Camilli, G., Williams, L., Graff, J., Zeig, J., Zmach, C., & Nowak, R. (2010). Addressing Summer Reading Setback Among Economically Disadvantaged Elementary Students. *Reading Psychology, 31*(5), 411–427. https://doi.org/10.1080/02702711.2010.505165 , accessed 2.4.2022.
- Convention on Cybercrime, European Treaty Series - No. 185.
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
- Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005)
- Council of Europe. (2021) Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment (Adopted by the Committee of Ministers on 28 April 2021 at the 1402nd *meeting of the Ministers› Deputies).*
- Council of Europe. (2018a) Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and

fulfil the rights of the child in the digital environment (Adopted by the Committee of Ministers on 4 July 2018 at the 1321 meeting of the Ministers' Deputies).
- Council of Europe. (2018b) Guidelines to respect, protect and fulfil the rights of the child in the digital environment - Recommendation CM/Rec(2018)7 of the Committee of Ministers (2018). Available at: https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digitalenvironment-recommendation-cmrec20187-of-the-committee-of-ministers.html, accessed 4.4.2022.
- Council of Europe. (2016) Council of Europe Strategy for the Rights of the Child (2016-2021) Children's human rights. Available at: *https://rm.coe.int/strategija-vijeca-europe-za-prava-djeteta-croatia/1680931c64*, *accessed* 4.4.2022.
- Council of Europe. (2014) Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies).
- Council of Europe. (2009) *Recommendation* CM/Rec(2009)5 **of the Committee of Ministers to member states on measures to protect children against harmful content and** *behaviour and to promote their active participation in the new information and communications environment (Adopted by the Committee of Ministers on 8 July 2009 at the 1063rd meeting of the Ministers' Deputies).*
- Council of Europe. (2008) *Recommendation* CM/Rec(2008)6 *of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters (Adopted by the Committee of Ministers on 26 March 2008 at the 1022nd meeting of the Ministers' Deputies).*
- Council of Europe. (2008) Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (Adopted by the Committee of Ministers on 20 February 2008 at the 1018th meeting of the Ministers' Deputies).
- Council of Europe. (2007). **Recommandation** CM/Rec(2007)11 **du Comité des Ministres sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication** *(adoptée par le Comité des Ministres le 26 septembre 2007, lors de la 1005e réunion des Délégués des Ministres).*

- Council of Europe. (2006) *Recommendation* CM/Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment *(Adopted by the Committee of Ministers on 27 September 2006 at the 974th meeting of the Ministers' Deputies).*
- Council of Europe. (2001). Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services) (Adopted by the Committee of Ministers on 5 September 2001 at the 762nd *meeting of the Ministers› Deputies)*.
- Degges-White, S. (9.11.2018). Are Parents to Blame for #GenerationLonely? *Psihology Today*. Available at: https://www.psychologytoday.com/intl/blog/lifetime-connections /201811/are-parents-blame-generationlonely, accessed 4.01.2022.
- European Court of Human Rights. (2022) Factsheet – New technologies. Available at: https://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf, accessed 16.4.2022.
- European Network of Ombudspersons for Children. (2019a) Position Statement on "Children's Rights in the Digital Environment" Adopted by the 23rd ENOC General Assembly, 27th September 2019, Belfast. Available at: http://enoc.eu/wp-content/uploads/2019/10/ENOC-2019-Statement-on-Childrens-Rights-in-the-Digital-Environment.pdf, accessed 6.4.2022.
- European Network of Ombudspersons for Children. (2019b) ENYA Recommendations Children's Rights in the Digital Environment. Available at: http://enoc.eu/wp-content/uploads/2019/10/ENYA-recommendations-on-childrens-rights-in-the-digital-environment-FV.pdf, accessed 4.4.2022.
- EUROPOL. (2019) Internet Organised Crime Threat Assessment (IOCTA) 2019. Hague: European Union Agency for Law Enforcement Cooperation. Dostupno na: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, accessed 4.4.2022.
- European Data Protection Supervisor. (2018) EDPS Opinion on online manipulation and personal data. Brussels: European Data Protection Supervisor. Available at: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf, accessed 6.4.2022.
- George, M., Jensen, M., Russell, M., Gassman-Pines, A., Copeland, W., Hoyle, R., & Odgers, C. (2020). Young Adolescents' Digital Technology Use, Perceived Impairments, and Well-Being in a Representative Sample. The

Journal of Pediatric 219(1), pp. 180-187, DOI: https://doi.org/10.1016/j.jpeds.2019.12.002, accessed 9.4.2022.
- Geldhof, E., Cardon, G., De Bourdeaudhuij, I., & De Clercq, D. (2007). Back posture education in elementary schoolchildren: A 2-year follow-up study. European Spine Journal, 16(6), str. 841–850, https://doi.org/10.1007/s00586-006-0227-4, accessed 4.4.2022.
- Global WebIndex. (2020). Coronavirus Research, Series 4: Media Consumption and Sport. Available at: https://www.gwi.com/hubfs/1.%20 Coronavirus%20Research% 20P DFs/GWI%20coronavirus%20findings%20April%20 2020%20%20Media%20Consumption%20(Release%204).pdf, accessed 4.4.2022.
- Harari, Y. (2015) *Homo Deus - A Brief History of Tomorrow*. London: *Harvill Secker.*
- Kimberly, M., Finkelhlor, D., Jones, L., & Wolak, J. (2010) Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization. *Journal of Adolescent Health 47*(2), pp. 183-190, https://doi.org/ 10.1016/j.jadohealth.2010.01.007, accessed 10.4.2022.
- Criminal Code of Republika Srpska, “Official Gazette of Republika Srpska”, 64/2017, 104/2018, 15/2021 and 89/2021
- Lalić, M. (8. Septembar 2020). Jesu li digitalne tehnologije zaista tako loše za metalno zdravlje tinejdžera? Medijska pismenost. Available at: https:// www.medijska pisme nost.hr/jesu-li-digitalne-tehnologije-zaista-tako-lose-za-metalno-zdravlje-tinejdzera/, accessed 5.4.2022.
- Lancioni, G. E., Sigafoos, J., O’Reilly, M. F., & Singh, N., N. (2013) *Assistive Technology: Interventions for Individuals with Severe/Profound and Multiple Disabilities*. New York: Springer Science.
- Livingstone, S., Blum-Ross, A., Pavlick, J. & Ólafsson, K. (2018) In the digital home, how do parents support their children and who supports them? Parenting for a Digital Future: Survey Report 1. Available at: https://www.lse.ac.uk/media-and-communications/ assets/ documents/research/preparing-for-a-digital-future/P4DF-Survey-Report-1-In-the-digital-home.pdf, accessed 4.4.2022.
- Marković, I. (2018) Seksualno zlostavljanje i iskorištavanje djece (novine u Krivičnom zakoniku Republike Srpske). *Godišnjak Pravnog fakulteta 40*(40), 27-43, DOI 10.7251/GOD1840027M.
- Mataušić, J. M. (2002). Utjecaj masmedija na obitelj, *Riječki teološki časopis,* 442-455.

- Mićević-Karanović, J. Ž., Mesaroš-Živkov, A. J., Pavlov, S. V. & Brkljač, T. S. (2020) Rizični uticaji digitalnih medija na psihofizički razvoj dece predškolskog uzrasta. *Sinteze,* 18, 33-53. https://doi.org/10.5937/sinteze9-22205, accessed 12.4.2022.
- Miladinović, A. (2018) *Bezbjednosni incidenti prema djeci na društvenim mrežama*. Banja Luka: Ministarstvo unutrašnjih poslova Republike Srpske.
- Murphy, S., Buckle, P., & Stubbs, D. (2004). Classroom posture and self-reported back and neck pain in schoolchildren. *Applied Ergonomics, 35*(2), 113–120. https://doi.org/10.1016/j.apergo.2004.01.001, accessed 12.4.2022.
- Odgers, C. & Jensen, M. (2020) Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions. *The Journal of Child Psychology and Psychiatry 61*(3), pp. 215-398, https://doi.org/10.1111/jcpp.13190, accessed 14.4.2022.
- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, Adopted 25 May 2000 by resolution A/RES/54/263 at the fifty-fourth session of the General Assembly of the United Nations.
- Odluka o ratifikaciji Fakultativnog protokola uz Konvenciju o pravima djeteta koji se odnosi na prodaju djece, dječiju prostituciju i dječiju pornografiju, Službeni glasnik BiH - Međunarodni ugovori, br. 5/2002.
- Orben, A. (2019) *Teens, Screens and Well-Being: An Improved Approach. Doctoral Thesis.* Trinity: University of Oxford. Available at: https://mwww.amyorben.com/docs/ thesis/_main.pdf, accessed 4.4.2022.
- Pavlović, D. & Vulić, T. (2014) Izazovi i perspektive novih medija u odnosu na tradicionalne. IN: Nedeljković Valić, D. & Pralica, D. (Ur.), *Digitalne medijske tehnologije i društveno-obrazovne promene 4.* Univerzitet u Novom Sadu, Filozofski fakultet, 155-164.
- Pylkin, A., Serkova, V., Petrov, M., & Pylkina, M. (2021) Information Hygiene as Prevention of Destructive Impacts of Digital Environment. In: Bylieva, D., Nordmann, A., Shipunova, O., Volkova, V. (eds) *Knowledge in the Information Society. PCSF CSIS 2020 2020. Lecture Notes in Networks and Systems*, vol 184. Springer, Cham. https://doi.org/10.1007/978-3-030-65857-1_4, accessed 15.4.2022.
- Rideout, V., Foehr, U. & Roberts, D. (2010). *GENERATION M2 Media in the Lives of 8- to 18-Year-Olds*. Henry J. Kaiser Family Foundation. Available at: https://files.eric.ed.gov/fulltext/ED527859.pdf, accessed 4.1.2022.
- Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, (no date).

- Straker, L., Pollock, C., Burgess-Limerick, R., Skoss, R., & Coleman, J. (2008). The impact of computer display height and desk design on muscle activity during information technology work by young adults. *Journal of Electromyography and Kinesiology, 18*(4), 606–617. https://doi.org/10.1016/j.jelekin.2006.09.015, accessed 4.4.2022.
- Stojanović, Z. (2018) *Komentar Krivičnog zakonika*. Beograd: Službeni glasnik.
- Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review, 8*(2) 1. DOI: 10.14763/2019.2.1410.
- Šikman, M. (2020) Transforativne tehnologije i kriminal (oblici ispoljavanja i mjere suzbijanja). U: Mirjanić, Ž. & Milinković, I. (Ur.) *Transformativne tehnologije: pravni i etički izazovi XXI vijeka*. Banja Luka: Pravni fakultet Univerziteta u Banjoj Luci, 233-248.
- Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. (2018) Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time. *Clinical Psychological Science, 6*(1), pp. 3-17, doi:10.1177/2167702617723376.
- UNICEF. (2017). Children in a Digital World - The State of The World's Children 2017. New York: UNICEF. Available at: https://www.unicef.org/media/48601/file, accessed 10.4.2022.
- Veljović, A., Vulović, R., & Damnjanović, A. (2009) *Informaciono komunikacione tehnologije u menadžmentu*. Čačak: Tehnički fakultet.

Akademik prof. dr Miodrag SIMOVIĆ,
potpredsjednik Ustavnog suda BiH i
redovni profesor Pravnog fakulteta Univerziteta u Bihaću i
redovni član Akademije nauka i umjetnosti BiH

Prof. dr Mile ŠIKMAN,
vanredni profesor Pravnog fakulteta u Banjoj Luci

UTICAJ DIGITALNOG OKRUŽENJA NA DJECU I REAGOVANJE NA DRUŠTVENO NEPRIHVATLJIVO PONAŠANJE

Uticaj digitalnog okruženja na psihofizički razvoj djece se sve više i dominantnije manifestuje, u prilog čemu idu i emprijski pokazatelji. Vrsta i stepen uticaja mogu da budu različiti, a posljedica je uvijek ista i ogleda se štetnim efektima na psihofizički razvoj djece. Istovremeno, mnogobrojne studije o žrtvama prikazuju da je stvarni uticaja visokih tehnologija na psihofizički razvoj djece mnogo veći, nego što je to iskazano putem dostupnih podataka. Osnovni razlog za takvo stanje mogao bi se tražiti u razlozima neprijavljivanja ovih ponašanja od strane žrtve ili bolje rečeno neprepoznavanje štetnih efekata visokih tehnologija na psihofizički razvoj djece. Na to možemo dodati štetne efekte sekundarne viktimizacije, kojom su vrlo često obuhvaćene žrtve krivičnih djela. U tom smislu postavlja se pitanje na koji način društvo može najadekvatnije reagovati na ova ponašanja. Različiti modeli prevencije mogu da daju obećavajuće rezultate, ali otvaraju pitanja zaštite dječijih prava, uključujući i lične podatke. S druge strane, krivičnopravna represija, kao ultima ratio ima puno opravdanje uvođenja, ali i znantna ograničenja. Upravo navedeno jeste predmet ovoga rada, a to je sprečavanje i suzbijanje društvenog neprihvatljivog ponašanja koje se manifestuje upotrebom visokih tehnologija, bilo da su djeca žrtve ili pak akteri ovih ponašanja.

Ključne riječi: digitalno okruženje, djeca, krivično djelo, generalne prevencija, specijalna prevencija.

Slađana JOVANOVIĆ, PhD*
Full Professor,
Union University Law School, Belgrade

Ljubinka MARKOVIĆ**
Juvenile Justice Counsellor
Higher Court in Belgrade

Original Scientific Article
Received: 8 February 2023
Accepted: 1 March 2023
UDK: 343.988:[316.624-053.6:004.-738.5(497.11)
https://doi.org/10.47152/rkkp.61.1.2

JUVENILE OFFENDERS AND VICTIMS OF DIGITAL VIOLENCE

The authors are focused on the issue of digital violence among juveniles: factors, main characteristics, and responses to it. The paper is primarily based on the latest research results of judicial practice (of the Higher Court in Belgrade and the Higher Prosecution Office in Belgrade – Special Department for High-Tech Crime), data gathered by questionnaires filled out by juveniles from one secondary school in Belgrade, and other available studies on the topic. Some recommendations regarding the social response to digital violence among juveniles were made, having in mind General Comment No. 25 (2021) on children's rights in relation to the digital environment adopted by the Committee on the Rights of the Child.

Keywords: juvenile offenders/victims, digital violence, social media/networks

* e-mail: sladjana.jovanovic@pravnifakultet.rs
** e-mail: ljubinka.markovic@bg.vi.sud.rs

1. Introduction

The general development of education, the availability of science and culture, and the development of humanity, in general, had two significant moments: the first one is Gutenberg's invention of printing machines, and the second one is like the Big Bang - the development of digitalization. The advantage of digitizing the achievements of knowledge, science, and art is indisputable: availability of real, but also macro and micro spaces and processes; direct transmission of all information and events (even at the moment when they happen), and meeting people from far away and communicating with those whose language we do not know, but with whom we talk through digital translators. Undoubtedly, social media have enormous benefits for the development of everyone, especially for children as it is also emphasized in General Comment No. 25 (2021) on children's rights in relation to the digital environment (Committee on the Rights of the Child, 2021).
Yet this new, digital world doesn't offer just benefits and advantages. The rules and regulations governing the digital world are still modest in relation to such a complex structure. In addition to useful content, even crime has "moved" to the digital environment, finding various opportunities to flourish. It is not always easy to determine whether the information in social media hides "devils in disguise "—false people and organizations, whether fake news is being presented, and whether malicious influences are exerted on consumers for the purpose of abuse. Statistics show that even skilled individuals and professional organizations can become victims of digital (high-tech) crime (73 Important Cybercrime Statistics, 2023). The following data (from July 2022) could be used as an illustration of the vast exposure to victimization: 63.1% of the world's population uses the Internet (Internet World Stats, 2023)[1] and more than half of Internet users (59%) are on social networks (Petrosyan, 2022). According to UNICEF data: one-third of Internet users are children (UNICEF, 2017), and as they grow older, their time online increases (Popadić et. al., 2016: 58; Kuzmanović et al., 2019: 14).

A comparison between the proportion of young people and the proportion of the whole adult population engaged in online activities across the EU in 2021 shows that the largest difference between these two groups was recorded for participating in social networks (Eurostat, 2022). The data of the European survey "EU kids online 2020" is of great concern as they indicate that Serbia is among

1 Serbia is a country with a higher number of Internet users than the average (above 70%). Alphabetical List of Countries - Internet Indicators - ISO3316 (internetworldstats.com), accessed on 15. 1. 2023.

the leading in the number of children under the age of 13 on social networks. Namely, the daily use of social networking sites among 12- to 14-year-olds varies between 10% (Finland) and 86% (Serbia and Russia). Also, the number of 15- to 16-year-olds who use social networking sites daily varies between 21% in Finland and 93% -in the Czech Republic and Serbia (Smahel et. al., 2020: 30).

Are children in the digital world like Alice in Wonderland? Once they enter that world of wonders, can they control further events, and resist all lures and challenges? Are they really free to choose? Can they refuse what they don't want? Can they be safe or free to get out when they want to, without consequences? The child's specific status makes her/him very vulnerable and exposed to various risks and victimization (or even criminalization) in the digital world. It is a huge task to protect children in the digital environment, to prevent the possibility of their victimization, and to help rehabilitate those who have already become victims. It is also necessary to prevent children from becoming bullies (or perpetrators of other offenses, e.g. offenses against the security of computer data) through digital media, as they offer great opportunities for those who would like to harm others in a swift, repetitive, impersonal way, from a very comfortable position.

The aim of this paper is to determine some of the phenomena related to the criminal aspect of the activities of juveniles on various social networks, to determine some of the risks, as well as the factors of child protection on the Internet and thus give guidance to the development of prevention programs. The starting point was the experience in criminal cases of the Higher Court in Belgrade (cases in which minors were victimized or committed criminal offenses[2]), whether criminal offenses were already defined as high-tech crime or digital media were among the means for committing criminal offenses. The experience of the Deputy Higher Public Prosecutor Mr. Aleksandar Momčilović (Department for the High Tech Crime of the Higher Public Prosecution Office in Belgrade) was of great importance.

2. Juvenile offenders and victims through digital media

Bullying of children and young people through digital/social media is very common within their peer communication. It is reflected most often in insulting

2 A juvenile offender is a person who at the time of commission of the criminal offence has attained fourteen years of age and has not attained eighteen years of age (Article 3, Paragraph 1 of the Law on Juvenile Criminal Offenders and Criminal Law Protection of Juveniles, Official Gazette RS, No. 85/2005).

and disparagement of one of the peers[3]. Although bullies “troll” more of their peers, they will more often take these actions continuously towards those who are most vulnerable and susceptible to the position of “victim”. As a rule (in fear of becoming targets of such abuse themselves), the bully is joined by others in the group, and the abuse takes the form of a public lynch. Very often, from violence on social networks, they switch to a “traditional” form of violence (psychological, physical, or sexual violence in the “real world”).

In the practice of the Higher Court in Belgrade, it could be noticed in cases prosecuted for crimes whose qualifications do not indicate the abuse through digital media (e.g. light/serious bodily injury, attempted murder, etc.) that the criminal offense was preceded by digital abuse of the victim. This is also the case with crimes such as endangering security, stalking, sexual harassment... behind which digital bullying is often hidden. There have also been cases in which a juvenile, after prolonged exposure to abuse through digital media/social networks, committed a criminal offense against the person (also a minor) who harassed, insulted, belittled him, or asked others in the group to “block” him in personal communication, or in front of everyone in the group - to exclude him from the group. Some researchers have determined the reverse sequence of events – “traditional” forms of violence were preceded by digital violence (Popadić, Kuzmanović, 2013: 8), but rarely – digital violence is the only form of violence (Modecki, 2014 according to Aleksić Hil, Kalanj, 2018: 63). Undoubtedly, there is a strong link between two forms of violence, supplementing or inducing each other.

In addition to these phenomena, cases of classic crimes in the field of high-tech crime have been recorded. Two cases are particularly interesting.

Case 1:

A seventeen-year-old boy, in company with an adult, committed the criminal offense of Computer Fraud under Article 301, paragraph 1, of the Criminal Code (hereinafter: CC)[4]. In a period of about 20 days, he obtained data on payment cards from the USA, obtaining them through an SQL exploit program that searches for unprotected databases of online customers, and then used them for payment when buying mobile phones, computers, and computer equipment, worth

3 More about children and hate speech on social networks: Pavlović (2022); Kubiček, Marković (2022).

4 Criminal Code, Official Gazette of the Republic of Serbia, Nos. 85/05 (Corrigendum), 107/05 (Corrigendum), 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 and 35/19.

more than 215,000 dinars. The minor designed the program himself and carried out computer fraud, registering under an assumed name.

Case 2:

A young adult, a first-year student of the Faculty of Mathematics, was tried before the Higher Court in Belgrade for the criminal offense of Creating, Obtaining, and Providing another Person with Means for Committing Criminal Offenses against the Security of Computer Data (Article 304a, paragraph 1 of the CC). It was established that the young adult committed the offense even before the age of eighteen. He (in the second grade of high school) made and sold computer programs for the purpose of committing criminal offenses against the security of computer data, by creating on his PC computer programs - "cryptors" that serve to hide a computer virus from antivirus programs, so that it would not be detected and deleted, i.e., to provide computer viruses and other malicious programs with an additional layer of protection, allowing the destruction, alteration, and theft of other people's data. The programs are intended for the commission of criminal offenses of Computer Sabotage (Article 299 of the CC), Creating and Introducing of Computer Viruses (Article 300 of the CC) and Unauthorised Access to Computer, Computer Network or Electronic Data Processing (Article 302 of the CC). He sold these programs through hacker forums "Darkode" and "Exploit.im".

Minors appeared before the juvenile council of the Higher Court in Belgrade for the purpose of committing the criminal offense of Showing, Procuring and Possessing Pornographic Material and Minor Person Pornography (Article 185 of the CC)[5]. In some cases, it was about recording voluntary sexual relations with a minor (most often a girl) and posting such videos on the Internet, but there was also recording and distributing violent sexual intercourse, and the proceedings were also conducted for the criminal offenses of Rape (Article 194 of the CC), Sexual Intercourse with a Child (Article 180 of the CC) or Prohibited Sexual Acts (Article 182 of the CC) with a minor as a victim. The above-mentioned is in accordance with UNICEF data showing that about *80%* of children in 25 countries report feeling in danger of sexual abuse or exploitation online. Indeed, the most alarming is the threat of online sexual exploitation and abuse of children, as it has never been easier for child sex offenders to contact their potential victims, share imagery, and encourage others to commit offenses (UNICEF, 2022).

5 More about this offense: Škulić, 2022.

3. Minor victims of digital violence and crimes related to digital media

Mr. Aleksandar Momčilović, Deputy Higher Public Prosecutor (Department for the High Tech Crime of the Higher Public Prosecution Office in Belgrade), informed the authors that although the Special Department for the High-Tech Crime does not have the exact number of minor victims, in almost all criminal offenses of Showing, Procuring and Possessing Pornographic Material and Minor Person Pornography (Article 185 of the CC) and Abuse of Computer Networks or other Technical Means of Communication for Committing Criminal Offenses against Sexual Freedom of the Minor (Article 185b of the CC)[6] the number of registered minor victims was between five and ten victims. The number of victims is likely significantly higher, but they were either undetected or the parents (and minor victims) were unwilling to participate in the criminal proceedings, denying their children had anything to do with the cases in question.

Table 1 provides data for the last five years on the number of cases of criminal charges for the aforementioned criminal offenses, filed in the Register of Known (Adult) Perpetrators (Special Department for High-Tech Crime).

Table 1: *Criminal charges (Art. 185 and Art. 185b of the CC: 2017 - 2021*

Year	2017	2018	2019	2020	2021
Art. 185	29	28	24	40	107
Art 185 b	4	4	-	-	-

According to Mr. Momčilović, these data represent only 10% of the aforementioned criminal offenses committed by unknown adult perpetrators.

Based on his experience, but also on the direct experience of the co-author - Juvenile Justice Counsellor of the Higher Court in Belgrade (who is directly involved in the preparation and support of juvenile victims and witnesses) it can be concluded that minor victims of these crimes are most often children vulnerable due to belonging to marginalized groups, children in residential accommodation in social protection institutions, but also children who, due to family and other circumstances, exhibit inappropriate behaviour, whether it is in the form of social isolation, behavioural problems, running away from home, alcohol and drug abuse or sexual and promiscuous behaviour. Most of them are girls[7].

6 More about this offense: Jovašević, 2022.

7 UNICEF survey shows the same. More in: UNICEF (2021) *Ending Online Child Sexual Exploitation and Abuse*, p. 13. See also: Csepregi, Kovács (2022).

Juvenile victims of criminal offenses committed using digital media, in addition to the aforementioned, take part in the proceedings conducted against adult perpetrators (and minors, too) such as: Rape (Article 178 of the CC), Sexual Intercourse with a Child (Article 180 of the CC), Endangerment of Safety (Article 138 of the CC), Sexual Harassment (Article 182a of the CC), Stalking (Article 138a of the CC), Coercion (Article 135 of the CC), Blackmail (Article 215 of the CC).

Minors often become victims of these crimes, mostly girls who do not come solely from the category of vulnerable groups. The following cases are good examples.

Case 3:

A 16-year-old girl accepts a Facebook friendship with a NN person. He was in a group with a friend of hers from a former elementary school. The usual correspondence lasts for several weeks. He says he's a year older than her. He lives in a town in western Serbia. He writes about school problems, his family, his friends, and the music he listens to. They exchanged photos. The young man liked her photos. He also tells her that he likes her. They start a virtual emotional relationship.

They exchanged photos in the swimsuits. He tells her that she is very handsome in a swimsuit and that he would like to see her naked. After a little persuasion, she photographed herself naked and sent a picture to him. He sends her a video of his genitals and masturbation. After that, she hasn't called him back for a few days. She said she was frightened and ashamed of their communication.

A classmate from the current class informs her that NN contacted her and asked for her (victim's) phone number. He said that if she didn't hear from him, he would send some of her photos to everyone in the group on Facebook.

Frightened, the girl reports the event. He tells her that no one can leave him unpunished. He orders her to come to his city to make love. She rejects him. He sends a video in which he vividly linked her nude photo to a video of a girl masturbating. He threatens to send her parents a video if she doesn't come to his town.

She's freaked out. She doesn't go to school for a few days, supposedly because of a headache. He begs NN not to do that and that he will be paid to delete the recording.

He gives her a bank-account number (it will later be determined that it is his own brother's account), and she pays him 24,000 dinars (the 200 euros she received for her birthday). After two weeks, he asks either to come or to pay him

again. The girl says she doesn't have money and will pay him when she collects it. He sends a nude photo of her to a friend and again threatens to send the arranged footage to her parents.

The juvenile goes to the police, reports NN, and asks the police not to insist that her parents be involved.

A swift response from the police, the high-tech crime department, revealed a 44-year-old man who had impersonated Facebook profiles as a 17-year-old boy. The criminal proceedings conducted for the criminal offenses of Coercion (Article 135 of the CC) and Blackmail (Article 215 of the CC), included the deletion of his account, as well as all contents he possessed.

Case 4:

A 26-year-old young man is on a new trial for the criminal offense of Endangering Security (Article 138 paragraph 1 of the CC), and Sexual Harassment (Article 182 paragraph 2 of the CC). He was previously sentenced to one year in prison for the same offense (waiting for the execution). A minor and her sister (also a minor), and three minor girlfriends were victims.

By impersonating his name and introducing himself as an 18-year-old boy through one of the multiple accounts he opened on Instagram, he approached a 16-year-old girl and asked if she could support him to boost the popularity of his profile. She advised him to change his profile photo first. After that, he tells her that it's important to him in order to keep his girlfriend. He sends photos of him and his alleged girlfriend. Benign communication lasts for some time. As the young man was extremely pushy and wrote continuously, day and night, an incredibly large number of messages, the girl blocked his account.

He contacted her from a new account, stating that he lived near her (provided her exact address), that he had already been "imprisoned" for raping a 12-year-old girl, and that he intended to do the same to her. A number of gruesome and vulgar threats followed, accompanied by detailed information about the school she attends, where she goes out, and whom she hangs out with.

At the same time, threats were made against her minor sister and her close friends (also minors).

After the girls told everything to their parents, the case was reported to the police. The defendant was taken into custody. All minors were questioned from a separate room, except for the sister who reached the age of 18. They all wanted to see what the defendant looked like, so they could recognize him if he was around them because they were seriously afraid of him.

It was determined that the defendant was suffering from paranoid psychosis. He was sentenced to compulsory psychiatric treatment and confinement in a medical institution and two years and four months in prison.

In both of these cases, people who met minors online were in virtual disguise. It was misrepresentation with the intentional aim of abusing another (minor) person.

How dangerous the occurrence of misrepresentation on social networks is, the so-called “catfishing” in some cases even with the help of serious visual scams such as “deepfake” can be seen in the recent past, when the victims became the mayors of Vienna, Berlin, and Madrid. Mayors, backed by teams of serious experts, negotiated and scheduled public talks, which were supposed to take place in front of television cameras, with a virtual person who identified himself as Vitali Klitschko, mayor of Kiev (Breaking Latest News, 2022, June 25).

One can only guess how many minors are threatened by this phenomenon.

4. Secondary school students as bullies and victims on social networks: research results

Based on the practice of the Higher Court and the Special Department (of the Higher Public Prosecution Office) for the High-Tech Crime in Belgrade and the observed (risky) behaviours of children on social networks, a survey was made to check whether these behaviours are common in the general population of underage adolescents. Students of the second, third, and fourth grades of one high school in Belgrade were surveyed (87 students).

Table 2 shows the structure of the sample by sex and age.

Table 2: *Sample structure by sex and age*

Age	15 years	16 years	17 years	18 years	Total
Girls	8	13	23	9	53
Boys	2	13	16	3	34
Total	10	26	39	12	87

The survey was conducted in May 2022, and some of the students reached the age of 18. Although they reached adulthood, their completed questionnaires are processed, because, essentially, their attitude towards the topic has not changed significantly compared to the period before adulthood.

4.1. The most commonly used social networks and applications for networking

The survey tried to determine on which platforms students most often make contacts with others, i.e. on which digital social networks they have “their own group” (Table 3). It is clear that there was no answer indicating the non-use of some platform for networking. The same results derived from other surveys (Popadić et al., 2016; Macanović, Stojanović, 2022: 112), while some show that even children aged 10 to 14 have their own profile on social networks (72,9% of primary school students (Kostić, Ranaldi, 2022: 90)).

It should be worth emphasizing that Serbia is among the leading countries in Europe in the number of children on social networks: the daily use of social networking sites among 12- to 14-year-olds varies between 10% (Finland) and 86% in Serbia. The number of 15- to 16-year-olds who use social networking sites daily is higher - in Serbia: 93%, in Finland: 21% (Smahel et al., 2020: 30).

Table 3: *The most commonly used social networks and applications*

Network/ Application	Girls 53 (100, 00%)	Boys 34 (100%)	Total 87 (100%)
Instagram	36 (29 - only this network) 67,92%	28 (23 - only this network) 82,35%	64 (73,56%)
WhatsApp	13 (only this network) 24,07&	6 (3 only this network) 17,65%	19 (21,84%)
TikTok	6 (5 only this network) 1,31%	3 (1 only this network) 8,82%	9 (10,43%)
Snapchat	3 (only this network) 5,66%	1 (2,94%)	4 (4,60%)
Viber		1 (only this network) (2,94%)	1 (1,15%)
Facebook	1 (1,89%)		1 (1,15%)
Twitter		1 (2,94%)	1 (1,15%)
Twitch		1 (2,94%)	1 (1,15%)
Discord	1 (1,89%)		1 (1,15%)
Pinterest	1 (1,89%)		1 (1,15%)
YouDude		1 (only this network) (2,94%)	1 (1,15%)

The most commonly used social network is Instagram, which is the most popular social network among younger children in Serbia (Kostić, Ranaldi, 2022: 93). Through this platform, 73,56% of total respondents realize their social net-

working (67,92% of girls and 82,35% of boys). WhatsApp (with a total of 21.84%) is followed by TikTok with 10.43% and Snapchat with 4.60%, while other networks/applications are used very sporadically.

The answers related to the social group on the platform are presented in Table 4.

Table 4: *Number of social groups, group size and knowledge of group members*

	Number of social groups	Number of group members*	Do they know each other in the group?*		
			All members are known	Most of them are known	Most of them are unknown
Girls 53	Number of social groups	14 (28%) up to 5 members 15 (30%) 6-10 2 (4%) 11-20 19 (38%) more than 20	40 (80% of 50 girls who are in group/s)	10 (20%)	–
Boys 34	Number of social groups	12(38,71%) up to 5 members 9(29,03%) 6-10 10(32,26%) more then 20	21 (67,74% of 31 boys who are in group/s)	10 (32,2%)	–

* comparisons are possible only in relation to those who are in one or more groups (50 girls and 31 boys).

Three girls (5,66% of all girls surveyed) and three young men (8.82% of all boys surveyed) crossed out group-related questions with the comment that they were “not in the group”.

The largest number of respondents communicate within three to six groups on social networks (16 girls, i.e. 30,19%, and 18 young men, i.e. 52,94%). Specifically, girls expressed a preference to have one (14 of them, i.e. 26,41%) or two (12, i.e. 22,64%) groups on digital networks (totalling 49,05%), while young men were inclined to have communication within more than seven groups (10 of them, i.e. 29,41%).

The percentage of those who are most often in very small groups (up to 5 members) was 28% of girls, and 38.71% of boys; in group/s counted more than 20 members was 38% of girls, i.e. 19 girls and 32.26%, i.e. 10 young men.

Although none of the respondents stated that he/she “doesn’t know the majority of the members” of the group or groups, many of them (ten girls, i.e. 20% and ten boys, i.e. 32,26%) do not know all members of the group, thus exposing themselves to risky communication and victimization.

4.2. Intragroup communication

Table 5 and Table 6 present answers to two important questions concerning the willingness to openly exchange personal experiences, attitudes, and thoughts in the group. On the one hand, this is a very important issue of freedom and respect for the rights and needs of all members of the group (certainly if communication is not violent and discriminatory for some). On the other hand, from a safety perspective, especially considering that 20% of girls and 32,26% of young men do not know all members of their groups and that they are often in large groups (38% of girls and 32,26% of young men), exposure to abuse on the social networks is increasing. It is interesting to point out that in the oldest age group, when the Internet is used most often generally, girls spend more time on the Internet than boys (Popadić et al., 2016: 58), thus making themselves more vulnerable and susceptible to risks and abuse.

Table 5: *Are you willing to share personal experiences on social networks?*

	Often	Sometimes	Never
Girls	9 (16,98%)	36 (67,92%)	8 (15,09%)
Boys	0	24 (70,59%)	10 (29,41%)

Nearly 30% of young men and 15% of girls never share experiences from their personal lives. About 17% of girls often share personal experiences with other members of a digital group. The largest number of both girls and boys (about 70%) occasionally share online experiences from their personal lives.

Table 6: *Are you willing to openly express your attitudes and reflections on social networks?*

	Often	Sometimes	Never
Girls	8 (15,09%)	24 (42,28%)	21 (39,62%)
Boys	6 (17,65%)	15 (44.12%)	13 (38,23%)

When it comes to attitudes and reflections, the distribution of answers is more fragmented. From the point of view of freedom of speech, it is concerning that almost 40% of both girls and young men never express their attitudes and thoughts. This can be the result of the heterogeneity of groups, the high fragmentation of the society in which we live, the desire to avoid conflicts, the lack of communication skills, and personal insecurity and fear of possible consequences.

But, this state of affairs, observed only for itself, still does not speak of safe behaviour on the Internet.

The answers to questions related to digital communication with strangers are presented in Table 7 and Table 8.

Table 7: *How often do you communicate with people you don't know personally?*

	Often	Sometimes	Never
Girls	5 (9,43%)	21 (39,62%)	27(50,94%)
Boys	7 (20,59%)	16(47,06%)	11(32,35%)

When it comes to communicating with strangers, young men have shown significant openness to girls: 20,59% of them often communicate with strangers, and 47,06% do so occasionally. More than half of girls say they never communicate on social networks with people they don't know personally. However, about 10% of girls communicate frequently with people they don't know, and nearly 40% do that occasionally.

There is a similar distribution of answers to the question of whether respondents easily accept acquaintances of their acquaintances and communicate with them about personal matters.

Table 8: *Do you easily accept acquaintances of your acquaintances and communicate with them about personal matters?*

	Often	Sometimes	Never
Girls	5 (9,43%)	22 (41,51%)	26(49,06)
Boys	6 (17,65%)	17 (50,00%)	11(32,35%)

4.3. Encounters with strangers, self-protection, and response to inconveniences

Risky behaviours, from the point of view of possible victimization, even by criminal offense, are certainly most pronounced in the fact that people, especially young people, and children, arrange encounters with strangers they have met on the Internet. In Tables 9 and 10, answers to questions related to the occurrence of direct dating with people known through social networks are presented.

Table 9: *Have you arranged an encounter with any of the unknown persons without the presence of people close to you?*

	Yes	No
Girls	24 (45,28%)	29
Boys	13 (38,25%)	21

Table 10: *How often does it happen?*

	Often	Sometimes	Never
Girls	0	24	29
Boys	3	10	21

A large number of young people occasionally had direct encounters with people they do not know personally, but whom they know virtually, through social networks (45,28% of surveyed girls and 38,25% of young men (one quarter of whom often made such contacts, and the rest of them - occasionally).

The largest number of respondents (when choosing a place to see a “virtual friend”) did not emphasize the aspect of personal safety, which does not have to be objective. It is possible that the cause is the discomfort to accept, at first, and then communicating personal fears and caution in planning and realizing such encounters. Most of the girls and young men point out that they jointly agree on the choice of place and time with a virtual acquaintance, taking into account when both are free, that the place is “halfway” or that it is close to them, and “that it is not boring”. Mostly, the place of encounter is familiar to them (café, park, etc.) or it is a cultural, entertainment, or sports facility, and meetings are arranged at the time of the concert, matches... A few girls have shown that when choosing a place to meet, they choose a place close to their home, where there are a lot of people, and some of them plan to meet in such a way that they are in close proximity to members of their peer group, pointing to the importance of personal safety.

To the question “Did you have any inconveniences, and if so, which?” 23 girls answered positively. Only two girls gave an incomplete answer to the question about inconveniences. In one case, “a friend of a friend was too pushy.” In the second, the girl “experienced tremendous discomfort, and her self-confidence for some things was shattered.” They did not specify in more detail what kind of harassment happened.

The girls who experienced some kind of harassment did not report it, but they talked about it with their friends.

The young men had no inconveniences from such encounters.

Table 11: *Experienced inconveniences when meeting a virtual acquaintance*

	Yes	No
Girls (24 realized such encounters)	23 (95,83%)	1
Boys (13 realized such encounters)	0	13

All respondents (both girls and boys) state that if they were harassed by a “virtual acquaintance”, they would talk about it with parents, friends, girlfriend/boyfriend, and psychologist. No one mentioned the National Contact Centre for Child Safety on the Internet, and no one has even heard about it[8]. E. Beković (from the Centre) said that there were 6304 reports on digital violence (since the foundation of the Centre in February 2017), assuming that the number of (unreported) cases must be much larger. Also, she told that the most frequent are cases of hate speech, and bulling by peers, as well as the fact that parents must be more educated and engaged in securing the safety of their own children on the Internet[9].

4.4 Prevalence of digital violence and response to it

Nearly 40% of girls surveyed say they have been harassed and subjected to violence on social networks or via text messages, e-mails, etc. Young men in almost twice as small numbers (20,59%) said they had such experiences (Table 12). Girls were more often cyber harassed than boys, which is in line with most studies (Fridh et al., 2015).

Table 12: *Victims of harassment/violence on social networks, via sms, e-mails…*

	Yes	No
Girls	21 (39,62 %)	32
Boys	7 (20,59 %)	27

Boys were most often harassed and exposed to violence on digital networks by peers, and girls by persons they knew, but who did not belong to their peer group (neighbours, relatives, friends of their friends...). The five girls said they suffered violence from different people (peers, acquaintances, and unknown persons). Table 13 provides data on persons who harassed minors.

8 National Contact Centre for Child Safety on the Internet was established in 2017, February 27 (based on the Regulation on the safety and protection of children in the use of information and communication technologies, Official Gazette of the RS, No. 61/16).

9 TV Prva, Morning: Child Safety on the Internet (guest: Emina Beković, National Contact Centre for Child Safety on the Internet) 8. 2. 2023.

Table 13: *Who are the persons who have harassed minors?*

	Peer	Another known person	Unknown person
Girls	8	14	10
Boys	4	1	2

The girls stated that they suffered harassment reflected in the public ridicule of their appearance, their attitudes, friends, and family members, the disclosure of their privacy, posting their pictures and images without permission (which they are ashamed of), belittling and verbal aggression, obscenity, giving pejorative and vulgar nicknames, but also being subjected to open sexual harassment, sending explicit images and videos, threats, and intimidation. They suffered continuous and frequent, even aggressive texting and emailing, and harassment over the phone and social networks. There were also allegations that they experienced "breaking into Instagram and impersonating a close person, then asking very intimate questions."

The young men said they experienced insults and disparagement, as well as psychological and sexual harassment. They did not specify in more detail the ways in which it was done. One of the young men said he was a "victim of a DDoS attack".

Most of the girls did not report cyberbullying. Only five girls who suffered serious threats and sexual violence on social media reported violence. Neither young man reported harassment in digital networking. Not even the young man who claimed to have been a victim of DDoS and probably suffered material damage as well. Table 13 presents the number of reported instances of digital harassment.

Table 14: *Who has reported digital harassment?*

	Yes	No
Girls	5	16
Boys	0	7

The five girls who reported harassment via social media did so by reporting it to their parents and one of them to the police (sexual harassment by an unknown). The answers for not reporting are: "I can solve the problem on my own (by blocking contact, and making the bully suffer in the same way)"; "I don't want to upset my family"; "I don't want to involve the police"; "He's a close person to me and I wanted to keep it between us"; "I had no one to report to." "I don't want to make any more trouble and draw others in"; "I don't want any further contact with that (unknown) person".

Most of the respondents stated that if they decided to report violence on social networks, they would do so by talking to their parents, friends, older friends, a psychologist, a pedagogue, a classmate, a teacher, and perhaps if the threats were serious, the police.

The answers to the question “If you know a peer who has been uncomfortable on a social network or otherwise through digital media, what was it about and did that person turn for help?” are also interesting. To this question, seven responded positively:

“My friend had a problem.”

“My friend had a problem, but she didn’t turn to anyone for help.”

“My friend’s profile was hacked, and she was bullied by an ex-boyfriend. She didn’t turn to anyone for help.”

“A close friend was threatened with death by a man, and he reported it to the police.”

“My friend was DDoSed. I helped him.”

“A lot of them were harassed. There were mostly insults or threats, but hardly anyone complains or seeks help because there are ways to block such people and solve the problem” - one of the male respondents said.

4.5 Committing digital harassment

When asked if they themselves were harassing someone, five girls (9,43% of the girls surveyed) said they harassed others digitally.

One girl said she was doing it out of “boredom.” She was reported to the police.

Another stated that she was doing it for fun. She didn’t want to hurt anyone, she just wanted to have fun. One of these girls created a fake profile and engaged in “teasing others”. One stated that “without identification, she grossly joked with a person close to her and then contacted her.” One of the girls allegedly sent inappropriate messages to a friend because she didn’t return her calls.

Four boys (11,76%) said they harassed others via digital media and social networks. None of them were sanctioned. They speak about the reasons for doing that (without specifying how they did it): “Because of the defence”; “Because that guy insulted the waitress”; “I harassed a friend for fun”; “I’ve been contacting my friends from a fake profile out of boredom and fun.”

Nine respondents said they knew about their peers who also committed digital harassment. They knew that some of their peers had serious quarrels and problems on social networks, some misrepresented themselves as if they were a

girlfriend of the friend they contacted and harassed, some posted inappropriate content and provocative photos and thus abused others, but they also knew that some of their peers/friends made programs that could harm others. None of them was sanctioned.

4.6. Analysis of Survey Results

The results of this survey are in line with others (mentioned above). Each student from the sample is involved in digital communication (on one or several social networks and/or using applications like Viber and WhatsApp) for networking. Almost 40% of girls surveyed and about 20% of boys were exposed to various forms of bullying through digital networking. Most often, the violence took place publicly, in front of all members of the group (in some cases, even outside the group).

Girls were most often subjected to insults, belittling, threats, and sexual harassment. The young men were also subjected to digital violence, which consisted of destroying part or the entire digital media/device. When it comes to girls, bullies were most often people they knew, but they were also harassed in significant numbers by peers and strangers. Young men were mostly harassed by peers or unknown persons. The young men did not report violence, while about one-quarter of the harassed girls reported the violence to their parents or friends. Only one girl, subjected to sexual harassment and threats, reported the violence to the police.

As reasons for not reporting violence, they pointed out that they can cope with the problem; they do not want to involve other people in the problem as if including others means their “connection” with the bully, whom they can simply ignore.

If they decide to report it, they would choose parents, friends, especially the elderly, teachers, psychologists, or pedagogues (schools), and eventually - the police.

About 10 % of respondents said they themselves harassed others, mostly in order to belittle them or to continue the conflict they have already had with the victim. Some considered it even a joke and fun, doing that out of boredom. They stated that some of their peers were victims of digital violence, even of very serious forms (threats to life, sexual harassment, destruction of a digital device, etc.).

The largest number of respondents communicate within three to six groups on digital networks. (30,19% of girls, 52,94% of boys). Nearly a third of young men communicate in more than seven groups, while girls are more likely to com-

municate in one or two groups (totalling about 50%). The number of those who were most often in very small groups, up to 5 members, was 28% of the girls and 38,71% of the boys. The number of those who were most often in the group/groups with more than 20 members was 38% of girls and 32,26% of boys).

Particularly alarming data indicating possible risks and victimization include the following: a significant number of respondents (20% of girls and 32,26% of boys) “do not know all members of the group”; 45.28% of girls occasionally had real encounters with people they do not know personally, but virtually, i.e. from social networks; 38,25% of surveyed boys had real and direct encounters with people they do not know personally, and almost one-quarter of them do so often, the rest only occasionally; out of a total of 24 girls who realized an immediate encounter with a virtual acquaintance, 23 of them stated that they experienced inconveniences during the encounter (they didn’t want to talk about what it was). Only two of the girls replied that they had received “blatant advances” and “something that shattered their self-esteem”. They talked about inconveniences just with their friends. Only a few girls have stated that they choose to be close to their home when meeting virtual acquaintances, or crowded places, and some girls said that they plan to meet in close proximity to members of their peer group, pointing to the importance of personal safety.

Presented data indicate a potential risk of victimization, especially considering the fact that about 70% of young people occasionally present experiences from their personal lives, thus revealing a lot in front of potential digital bullies and even “predators”, who often gladly use infiltration into large groups.

5. Concluding Remarks

As our and other (aforementioned) surveys show, along with benefits and progress, the digital age (and especially digital networking) has brought many risks and harms, opening up space for specific forms of criminalization and victimization. It can be concluded that a significant part of the social life of children and young people has moved to the digital world. So, they are particularly vulnerable to the risks that digital communication carries, given the time they spend in the digital world, inexperience, gullibility, and insufficient education about “digital culture”, risky behaviours, and consequences.

“Digital socializing” not only dominates as a form of socializing but also significantly affects the further development of children and young people. It is certainly not unexpected, given the development of technologies and the general lack of time for direct socializing, both due to the constant increase in obligations

of parents and children themselves, and because of the large part of the time that they spend (passively) using various digital media for the transmission of images, sound, and text.

The nearly three-year presence of the COVID-19 virus and epidemiological measures, which included online teaching, has further accelerated the shift of everyday and direct social communication, involving the shift from most physical contacts to digital platforms. This type of communication, when it becomes dominant, significantly impoverishes the emotional, social, and even moral development of children and young people. Cognitive development in such circumstances is also questionable. At first sight child/young person has a large amount of information, even a good structure for their connection and cause-and-effect relationships, but cognitive operations are often unthinkable without the use of modern technologies.

In the digital world, everything seems more simplified and lasts shorter than in the real world. In the real world, we see a lot more. In understanding an event or behaviour, we perceive in great detail, consciously or unconsciously, and then select sequences that will contribute to recognizing, knowing, and understanding the experienced, thus directing and guiding our behaviour. The presentation on digital platforms is “what someone else wanted us to see.” We do the same ourselves. We post our most beautiful footage and photos on the networks, we show ourselves how we want others to see us. Not all communications are and need not be like this. But there is a huge space for misrepresentation, manipulation, and misuse of digital media.

The answers obtained through our survey and the examples and experiences from criminal cases of the Higher Court and the Higher Public Prosecution Office in Belgrade indicate that young people (and also the children under the age of 15, who were not part of the survey sample), in order to protect their safety, the right to development and the right to freedom, must have better preparation and education in the sphere of digital social networking.

The proper attitude of the child in a digital environment is the basis for protection from possible abuses that lurk in the virtual world. The “good servant, evil master” approach is also very applicable to digital platforms. Loneliness, alienation, and consequently some developmental problems, which arise when real, immediate physical gatherings of children and young people are replaced by virtual ones, were not the topic of this paper, but we must not forget them. Digital communication must be only a small part of interactions between people, especially within the children’s world. The preparation and education of parents for

the care and upbringing of children must include a clear attitude towards the presence of digitalization in the child's life and development.

Modern education must include the education of children in order to intensively but safely use the achievements of digitized knowledge and the benefits of unlimited digital communication. Teaching them to distinguish between the real and the virtual, to recognize dangerous situations, to know whom to turn to for help, and how they can protect themselves. Teaching them not to replace the real everyday world and socializing with virtual ones. Adequate training and education must also be directed to parents, teachers, educators, and everyone else who cares for children, which is the focus of regulations and recommendations such as the Regulations on the safety and protection of children in the use of information and communication technologies of the Government of the Republic of Serbia and General Comment No. 25 (2021) on children's rights in relation to the digital environment (UN Committee on the Rights of the Child, 2021).

Protecting children on digital platforms also includes some aspects that require them to be part of a completely separate work, but they should be mentioned. Children/juvenile offenders and victims of criminal offenses in the Republic of Serbia have a special status from the aspect of legal regulations and application of modern digital media, whether it is data management through electronic registers, hearing through audio-video techniques, or the digital presentation/exposure of data on an event in which the child is an actor or passive participant by the media (or even their parents or other persons close to them). Respecting these legal guidelines and sanctioning their violation in everyday practice should be the subject of a special survey.

References

- Aleksić Hil, O., Kalanj, M. (2018) Bulling and Mental Health. *Psychiatry Today*, *50*(1), pp. 59-66.
- Breaking Latest News (2022, June, 25) Deepfake, the mayors of Berlin and Vienna also deceived: they thought they were talking in videocall with their counterpart from Kiev, Deepfake, the mayors of Berlin and Vienna also deceived: they thought they were talking in videocall with their counterpart from Kiev-breakinglatest.news-Breaking Latest News, accessed on: 15. 1. 2023.
- Csepregi, K., Kovács, I. (2022) Online Sexual Exploitation of Children, in particular the Crime of Child Pornography, *Journal of Criminology and Criminal Law*, *60*(1) pp: 7-24. https://doi.org/10.47152/rkkp.60.1.1

- Criminal Code, Official Gazette of the Republic of Serbia, Nos. 85/05 (Corrigendum), 107/05 (Corrigendum), 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 and 35/19
- Eurotstat (2022) Being young in Europe today - family and society - Statistics Explained (europa.eu), accessed on: 18. 1. 2023.
- Fridh, M., Lindström M., Rosvall, M. (2015) Subjective health complaints in adolescent victims of cyber harassment: moderation through support from parents/friends - a Swedish population-based study. *BMC Public Health*. 2015, ortSep 23;15:949. Doi: 10.1186/s12889-015-2239-7. Available at: Subjective health complaints in adolescent victims of cyber harassment: moderation through support from parents/friends - a Swedish population-based study (nih.gov), accessed on: 18. 1. 2023.
- Important Cybercrime Statistics: 2023 Data Analysis&Projections, 73 Important Cybercrime Statistics: 2023 Data Analysis & Projections - Financesonline.com, accessed on: 15. 1. 2023.
- Internet World Stats (2023) Alphabetical List of Countries - Internet Indicators - ISO3316 (internetworldstats.com), accessed on: 15. 1. 2023.
- Jovašević, D. (2022) Encuraging Sexual Abuse of Minors through Computer Devices. *Journal of Criminology and Criminal Law*, 60(2), pp: 133-147. https://doi.org/10.47152/rkkp.60.2.6
- Kostić, J., Ranaldi, V. (2022) Social Peer Violence in the Digital Environment – Students' Attitudes and the Possibility of Prevention. In: I. Stevanović, M. Kolaković-Bojović (Eds.) *Children and the Challenges of the Digital Environment*. Belgrade: Institute of Criminological and Sociological Research, pp. 83-96.
- Kubiček, A., Marković, A. (2022) Hate Speech towards Roma Children in Digital Space: Discourse Analysiss of Users' Comments. In: I. Stevanović, M. Kolaković-Bojović (Eds.) *Children and the Challenges of the Digital Environment*. Belgrade: Institute of Criminological and Sociological Research, pp. 65-82.
- Kuzmanović, D., Zlatarović, V., Anđelković, N., Žunić-Cicvarić, J. (2019) *Children in Digital Age: Guidelines for Safe and Constructive Use of Digital Technology and the Internet*, Child Rights Centre of Užice.
- Law on Juvenile Criminal Offenders and Criminal Law Protection of Juveniles, Official Gazette of the Republic of Serbia, No. 85/2005.
- Macanović, N., Stojanović, R. (2022) Cyberbulling as a Form of Peer Violence in Schools. In: I. Stevanović, M. Kolaković-Bojović (Eds.) *Children*

and the Challenges of the Digital Environment. Belgrade: Institute of Criminological and Sociological Research, pp. 97-116.
- Modecki, K.L., Minchin, J., Harbaugh, A.G., Guerra, N. G., Runions, K. C. (2014) Bullying prevalence across contexts: a meta-analysis measuring cyber and traditional bullying. *Journal of Adolescent Health*, *55*(5), pp. 602-611. doi: 10.1016/j.jadohealth.2014.06.007
- Pavlović, Z. (2022) Children and Hate Speech on Social Networks. In: I. Stevanović, M. Kolaković-Bojović (Eds.) *Children and the Challenges of the Digital Environment*. Belgrade: Institute of Criminological and Sociological Research pp. 55-64
- Petrosyan, A. (2022) Worldwilde digital population, available at: Internet and social media users in the world 2022 | Statista, accessed on: 17. 1. 2023.
- Popadić, D., Kuzmanović, D. (2013) Utilisation of Digital Technologies, Risks and Incidence of Digital Violence among Students is Serbia. UNICEF: Belgrade. Available at: Microsoft Word - Digital Violence Summary.eng.docx (unicef.org), accessed on: 17. 1. 2023.
- Regulation on the safety and protection of children in the use of information and communication technologies, Official Gazette of the RS, No. 61/16.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries.* EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo
- Škulić, M. (2022) Criminal Law Reaction to Child Pornography/Juvenile Pornography -realized/created by Abuse of Computer Network/Communication by Other Technical Means. *Journal of Criminology and Criminal Law*, 60(2), pp: 9-57. https://doi.org/10.47152/rkkp.60.2.
- TV Prva, Morning : Child Safety on the Internet (guest: Emina Beković, National Contact Centre for Child Safety on the Internet) 8. 2. 2023. Available at: Jutro - 08.02.2023. (prva.rs), accessed on: 8. 2. 2023.
- UN Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25.
- UNICEF (2017) *Children in Digital World: The State of the World's Children*. New York: UNICEF, United Nations Children's Fund.
- UNICEF (2021) *Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries*. New York: UNICEF, United Nations Children's Fund.
- UNICEF (2022) *Protecting Children Online*. New York: UNICEF, United Nations Children's Fund.

Milana PISARIĆ, PhD*
Assistant
University of Novi Sad
Faculty of Law

Review paper
Received: 8 March 2023
Accepted: 12 April 2023
UDK: 343.14:004.056.53
https://doi.org/10.47152/rkkp.61.1.3

THE USE OF HACKING TECHNIQUES FOR THE PURPOSE OF CRIMINAL PROCEDURE

Since certain trends in information technologies significantly hinder criminal investigation, there is an evident need for the creation of an appropriate criminal procedure mechanism to overcome these obstacles. One of the options is to enable the law enforcement agencies to use hacking techniques in order to gain access to protected computer systems, networks and data, even remotely, in order to identify suspects, to monitor their activities and communications, and to collect evidence. In this paper the author is considering the possibilities, advantages and risks of using hacking techniques for the purposes of criminal proceedings. After pointing out the risks of malware use by the competent authorities, the normative framework for overcoming those risks was considered through regulating the authorized access to a protected computer system or network, as a special investigative action, so the data obtained through such actions could be used as evidence in the court of law.

Keywords: criminal procedure, electronic evidence, encryption, lawful hacking.

* E-mail: mpisaric@pf.uns.ac.rs

1. Introduction

Certain trends in the development of information technologies, especially those used to protect the privacy and security of computer systems, networks and data of legitimate users, also benefit the perpetrators of criminal acts, and have led to the fact that the state authorities responsible for detecting and proving criminal acts face with serious obstacles when they need to collect data from such protected systems and networks (Going dark problem, Pisarić, 2020). These tendencies have an extremely negative effect on the practical and technical ability of competent authorities to implement certain investigative measures and actions: a) providers of electronic communication services incorporate, as a default setting, encryption (increasingly end-to-end encryption, E2E) into their products and services - which makes it impossible to carry out covert surveillance of communications (Pisarić, 2022); b) manufacturers and users increasingly apply full disk encryption - which makes it impossible to search the device (Pisarić, 2021:); c) the use of hidden services in the dark web makes it impossible to identify devices and perpetrators;[1] d) the widespread use of mobile devices based on cloud computing makes it difficult to search them and collect computer data in the traditional way;[2] e) the widespread use of wireless networks makes it difficult to conduct covert surveillance of communications conducted at a single network access point, etc. In order to create a balance between technological development and the necessity for competent state authorities to respond adequately, it is quite justified for the legislator to create a legal framework for the collection of electronic evidence despite and in addition to technologies aimed at protecting security and privacy. One of the possible solutions is the mechanism of exceptional access (backdoors), which implies that device manufacturers/service providers are obliged to create an entry point in the device or network for accessing the necessary data without the knowledge and permission of the user (Pell, 2016: 609) Considering that in this way the entire computer system would be weakened, which is the unanimous opinion of the scientific and expert public in the field of information security (Abelson et al., 2015), we should not lose sight of alternative sources of data, which can be used without compromising the protection mecha-

1 In the Tor network, the privacy and security of the IP address, location and usage data of individual users are protected, as well as the privacy and security of the IP addresses of web servers, which host web pages and are called hidden services. In this way, an anonymous, encrypted connection is established - neither the user's IP address is known to the website, nor the server's IP address to the user.

2 Cloud computing service means storing device content on remote servers of the service provider (which are spread around the world) and accessing that content from any device and place with an appropriate connection (e.g. iCloud, Google Drive, OneDrive).

nisms of encryption (Kerr, 2018). Data stored in the cloud,[3] electronic communication metadata,[4] IoT device metadata,[5] etc. most often are not encrypted and represent a significant source of information for the work of law enforcement agencies, without the need to gain access to content protected by encryption. In addition, the legislators of certain countries have regulated the authorization of competent authorities to gain access, that is, to hack into a protected computer system/network (policeware, govware).

2. Malware-based hacking technique

Hacking means gaining access, through manipulation, to a computer data, program, system or network, which is done without the awareness, knowledge, consent and permission of the owner, or user. Access and manipulation are realized by overcoming protection measures in the computer, computer network or electronic data processing, most often by using malicious software, or malware, which is installed on the device in situ, or remotely.[6] Malware is a program code that is based on the exploitation of vulnerabilities, i.e. defects in the software and hardware elements of a computer system/network, which enable an unauthorized person to gain access and undertake activities in a protected computer system or network without the knowledge and consent of the user (often covertly). These vulnerabilities are exploited by using malware locally on the system being attacked (hands-on), or remotely (drive-by) (Bellovin et al., 2014: 23). The most effective use is a zero-day vulnerability, which is detected and exploited before the public or the manufacturer becomes aware of it due to system compromise.[7] There is a whole vulnerability market: the “white” market, where device and application manufacturers or other interested parties are offered vulnerabilities in the amount of several hundred thousand dollars and more, while they, in turn, in order to increase security and protect user privacy, offer monetary rewards for

3 As the content is usually stored in a decrypted form, the competent authorities can request the providers of this service to hand over the necessary data.

4 Metadata is information about electronic communication data, not including the content of the communication. Metadata refers to device location data, IP address of the sender or recipient, etc.

5 The Internet of Things are devices and sensors connected to the Internet or another computer network, such as smart TVs, GPS devices, etc.

6 Malware can be in the form of virus, worm, spyware, ransomware, key logger, etc.

7 Vulnerabilities can be categorized in several ways, and one of the divisions is between vulnerabilities that are known to the manufacturer (n-day vulnerabilities: n-days/old days) and vulnerabilities that are not known to the manufacturer (zero-day vulnerabilities: zero-day/0- days). The process of turning an n-day vulnerability into a zero-day vulnerability is called disclosure.

finding and reporting bugs (bug bounties);[8] the “black” market where vulnerabilities are offered and bought to gain illegal and unauthorized access to the system/network; the “grey” market, where the buying and selling of vulnerabilities takes place between government authorities and individuals and companies that offer products and technologies that are based on the exploitation of vulnerabilities (Anstis, 2021:4).

Unauthorized infiltration into electronic data processing, computer system or network, and access to data stored in the system or transmitted through the network, is undertaken in order to cause damage and/or take control over computer data, system or network. As such, hacking constitutes a criminal act, unless there is appropriate authorization for such an act. Authorization to competent authorities to use hacking techniques (right to hack back) can be given in order to achieve different goals.[9] For the purposes of criminal proceedings, the goal of hacking would be to enable the identification of devices and users in order to discover the perpetrator, or covert surveillance of communications, or search of a device, i.e to enable the obtaining of electronic evidence. In order to understand how this goal can be achieved, it is first necessary to show how hacking using malware takes place. The use of this technique takes place through four stages (Mayer, 2018:583):

1) Malware injection - Competent authorities can install malware in a device via portable hardware (USB, CD) after achieving covert, physical access to the device (in situ), or deliver it remotely to a target szstem/network, in several ways. The phishing technique is aimed at certain users, by “luring” them through a message to download content or visit a website infected with malware, which is then secretly installed in the device (drive-by-download). In the investigation of anonymous online activities, especially hidden services on the dark web, the watering hole technique can be used, which is aimed at all users

8 Companies such as Zerodium and Exodus Intelligence buy zero-day vulnerabilities from hackers and sell them to device manufacturers, law enforcement and security agencies. Monetary fees for a reported vulnerability depend on the operating system, device, application, and type of vulnerability. The highest sums are offered for vulnerabilities in the latest versions of the Android and iOS operating systems - up to two and a half million dollars, and in messaging applications - up to one and a half million dollars for the iMessage and WhatsApp applications.

9 Those goals could be: exercising control over messages (preventing message sending, manipulation of the domain name system, changing the content of the message, “flooding” communication channels, changing the face of the website), causing damage to a certain number of subjects (internal and external modification of physical systems and devices, data modification, service theft), conducting surveillance or collecting data and information (compromising the end device or host, monitoring the communication channel, “breaking” encryption). More on that, Access Now, 2016: 11-12.

who exhibit certain behavior. Namely, after the incriminating website is identified, the competent authorities take control of the server, in order to deliver malware that will exploit vulnerabilities in the browser, after which the malware infects every device whose user visits or logs in to a certain website;

2) Vulnerability exploitation - For the launch and execution of any downloaded/installed software in the computer system, there are certain security restrictions, i.e. the operating system assigns limited permissions to the software so that it can only access certain data and functionalities in the device, thus protecting the user's privacy and security (sandbox). In order for the law enforcement agencies to gain access to the necessary data, it is necessary to overcome these security obstacles, which is why the introduction of malware into the system is followed by the exploitation of vulnerabilities;
3) Task execution - After the security obstacles are bypassed, by exploiting the vulnerability, the malware now equipped with the necessary access permissions, is launched, takes (partial) control over the device and executes the task, i.e. collects data;
4) Reporting - After the launched malware has completed the task, or while the execution is still in progress, the collected data is sent to the server of the law enforcement agencies.

For the purposes of criminal proceedings, malware can be entrusted with a variety of tasks.

If it is necessary to collect data about a user who anonymously uses certain services, the malware collects identifying data about the device and the network (e.g. IP address, MAC address, type and version of the operating system, type and version of the browser, username, URL of the last visited web pages, etc.) and sends them to the server of competent authorities. This data is then used to relate a specific user to a specific device - when a specific IP address is identified, with the help of an Internet access service provider, a specific activity in the online environment is associated with the account, then a specific device associated with that account is identified through the MAC address, and then the user can be identified through the user name that was logged in at a certain time on that device.

Also, the malware can collect data from the device about wireless access points, which are then compared with the external database of service providers, and in this way the physical location of the device can be determined.

Malware can be used to gain access to a device and to collect content stored on a device (thus allowing for covert and remote device search and seizure of

electronic evidence) or data needed to log into a social network account, but also to take control of a camera or microphone (thereby enabling covert surveillance, tracking and recording).

In addition, it is possible for the achieved control to spread from the initially infected device (e.g. computer) to other devices connected to it (e.g. mobile phone) of the same user.

Finally, even when it comes to communication protected by E2E encryption, the use of malware allows the covert surveillance of the communication to be carried out on the end device before being encryped and sent, i.e. after being received and decrypted (Pisarić, 2022).

3. Examples of LEAs using malware-based techniques

Although hacking for the purposes of criminal proceedings has been the subject of a current debate on encryption in the general, professional and scientific public since 2015, as a factor that seriously threatens the criminal investigatoin, there are examples of the use of malware for the purposes of criminal proceedings from an earlier period. Beginning in the late 1990s, authorities in the USA used the Carnivore tool for monitoring traffic in the computer network (the so-called network sniffer) for investigative purposes (Hartzog, 2002). The first known case of the use of malware to overcome the encryption problem dates back to 1999: after searching the suspect's computer, an incriminating file was found, protected by the PGP encryption program, so the police, after receiving approval, secretly installed the KLS (Key Logger System) malware on the computer, which monitored and recorded everything keyboard inputs, including the PGP key code (Carrell, 2002).

Unlike these cases where the malware was physically installed on the suspect's device, in the 2000s malware is starting to be delivered remotely via a computer virus. The FBI first disclosed the use of this technique for remote computer searches in 2003: in Operation Trail Mix, the KLS malware, called Magic Lantern, was used to overcome the problem of protecting the communications of suspects using the PGP program (Curran et al., 2007: 309). In the Timberline case in 2007, the FBI remotely, using the phishing technique, installed the CIPAV[10] malware on the suspect's computer, which collected and sent the necessary data

10 Computer and Internet Protocol Address Verifier.

to their server,[11] on the basis of which the user's data was requested from the Internet access service provider.

It is also known that a malware has been used against an unspecified number of users through the watering hole technique in several cases so far: (a) in Operation Torpedo, 2012 – after the Dutch police gained access to the account of the administrator of a hidden service in Tor (Pedo Board) and located the IP addresses of servers in the USA that hosted a site with child pornography, the FBI was authorized by a court order to install malware (which was based on the exploitation of vulnerabilities in the Adobe Flash Player plug-in for the Tor browser) on hidden services and to apply the network investigative technique (NIT technique) in relation to each computer that accesses that service;[12] (b) in Operation Freedom Hosting, 2013 - the FBI, in cooperation with the French police, applied this technique to users of the Freedom Hosting server that hosted hidden services in the Tor network, including 23 websites with child pornography, by exploiting a vulnerability in the Mozilla Firefox browser in order to collect the IP and MAC addresses of service users;[13] (c) in Operation Pacifier, 2015 – after identifying and taking over the server hosting Playpen, a child pornography site, the FBI, authorized by a court order, continued to host the site for several weeks and, using the NIT technique, collected data on more than 8,000 user computers.[14] In all these cases, after collecting identifying data for individual computers, the police requested information about device users from Internet access service providers.

These examples of hacking by the competent authorities are not isolated precedents, and show that in the last twenty years the possibility of hacking has

11 CIPAV collected IP and MAC address, data about operating system, the browser used, registered computer users and registered computer name, as well as browsing history. More on that, Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account “Timberlinebombinfo” and Opening Messages Delivered to That Account by the Government .

12 More on that, Application for a Search Warrant, *In re* Search of Computs. that Access the Website “Hidden Service A” Which Is Located at oqm66m6lyt6vxk7k.onion, No. 8:12MJ360 (D. Neb. Nov.19, 2012); Application for a Search Warrant, *In re* Search of Computs. that Access the Website “Hidden Service B” Which Is Located at s7cgvirtswvojlis.onion, No. 8:12MJ359 (D. Neb. Nov. 19, 2012); Application for a Search Warrant, *In re* Search of Computs. that Access the Website “Bulletin Board A” Located at http://jkpos24pl2r3urlw.onion, No. 8:12MJ3 56 (D. Neb. Nov. 16, 2012).

13 More on that, Application and Affidavit for Search and Seizure Warrant, In the Matter of the Search of the computers that access “Websites 1-23”.

14 More on that, Application and Affidavit for Search Warrant, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89.

expanded - from the physical installation of “spy” software on a single device (spyware) to the mass infection of devices remotely. In addition, the use of hacking techniques by the law enforcement agencies has contributed to the development of the market for vulnerabilities and hacking products and services. In the future, it is entirely possible for authorities to send commands to a targeted device/ network/account from a central management server, or to require software vendors to include malware in a software update. Although the use of the mentioned and similar techniques should not be denied a priori to competent authorities, the question arises whether it can be justified only by the technological reality of a complex IT environment, i.e. existing and new problems, on the one hand, and techniques for overcoming them, on the other hand. Namely, one must not lose sight of the invasiveness of the hacking techniques described, which implies the potential indiscriminate collection of data. In addition, there is a likelihood that their application will disrupt and/or cause damage to the wider information infrastructure. In other words, the application of hacking techniques by the competent authorities carries with it certain risks.

4. Risks of LEAs using malware-based techniques

At a time when looking for a way to provide LEA the access to protected communications, platforms and devices, prescribing the authorization for the use of hacking techniques, as a way to overcome the problem created by the application of technologies aimed at protecting privacy and security, is a better solution compared to the deliberate creation of new security flaws in the computer system/ network, in the sense of the Backdoor option (Pisarić, 2022:66). Nevertheless, the use of malware that is based on the exploitation even of existing vulnerabilities is not without risks, which can be additionally contributed to by the absence of clear and precise technical and legal rules.

A. Information security risk. The use of malware to gain access to a device/ system/ network carries with it a risk to information security, which goes beyond the specific target and potentially endangers the wider information infrastructure, because it is based on the discovery and exploitation of vulnerabilities. Especially the use of zero-day vulnerabilities creates risks, because they can appear in any software/ hardware, remain undetected for several months, even years, and are not easy to spot. The failure of competent authorities to disclose perceived vulnerabilities to software or hardware manufacturers contributes to the reduction of the general level of information security. Al-

though such an omission of disclosure may be justified by the interests of a specific investigation (but at the same time it allows the LEAs to repeatedly use zero-day vulnerabilities until they are discovered), it essentially makes it impossible for the manufacturer to overcome, i.e. “patches” vulnerabilities, putting all software/hardware users at risk. Also, there are known examples of vulnerabilities that were originally used by the competent authorities getting out of control, that is, they were discovered and used by malicious actors (e.g.: Stuxnet, Petya/Notpetya ransomware, Wannacry ransomware). The mentioned risks could be overcome by creating a system for managing vulnerabilities and prescribing strict legal and technical rules for their exploitation (such as exists, for example, in the USA - Vulnerability Equities Process).

B. Human rights risk. The LEA’s use of hacking techniques is extremely invasive and represent a potential disproportionate interference in individual human rights guaranteed at the international, regional and national level, primarily the right to privacy. With its application, it is possible to collect unlimited data that is stored in the device or transmitted over computer networks, both in relation to the suspect and in relation to legitimate users. As the challenge of detecting the suspect is the principle justification for the introduction of this investigative technique, and as the device used cannot be identified with certainty, there is a real risk that the malware may accidentally compromise the device/data of third parties. This is also contributed by the fact that this technique is to some extent indiscriminate, and that the target can be other users who share the targeted device, system or network. Also, the data obtained from the target device/network may contain sensitive, confidential, even legally privileged or proprietary material. The mentioned risks should be overcome by the norms of criminal procedural law.

C. Extraterritoriality risk. The transnational structure of the Internet, as well as the use of cloud services, require the competent authorities to act extraterritorially in certain cases in order to achieve remote access to computers/networks located abroad (Pisarić, 2016). However, the implementation of authorized hacking in the event that the targeted system/network or user is located outside the jurisdiction of the state where hacking would be permitted, would be contrary to the jurisdictional rules established by international public law (Pisarić, 2019: 228-231). Although it seemed traditional notion of state territory would

become irrelevant in cyberspace and that states could unilaterally prescribe the possibility of extraterritorial action to collect electronic evidence, the use of mechanisms for providing international assistance in criminal matters remains imperative, despite these procedures are slow and impractical. In this sense, it is necessary to improve the rules on mutual assistance in criminal matters in the collection and exchange of electronic evidence.

In order to find a balance between the interests of the criminal procedure and the interests of information security and privacy, it is necessary to create an appropriate legal framework for the use of this investigative technique, taking into account the mentioned risks, and in order to mitigate them, i.e. reduce them to the smallest possible extent. In the following part, the key requirements, to which the regulation of authorized hacking should be addressed, are considered.

5. Authorized access to protected computer system/network

The malware-based hacking techniques could be used to gain access to a protected computer, computer network, or electronic data processing in order to gather evidence. However, it is important to point out the difference between the two cases of hacking by the authorities.

In the first case, malware would be installed remotely into the device in order to gain access to the stored data (in order to remotely search the device and record/remove data) or data transmitted through the network (in order to secretly monitor communication on the end device, i.e. while it is in decrypted form).

In the second case, hacking techniques would be used to achieve access to a device protected by encryption and the data stored in it, which is physically accessible to the competent authority (in order to search the device in situ).

Considering the different degree of intrusiveness, the legal regulation should make a clear demarcation of the use of hacking techniques in these two cases, while taking into account a number of important and complex legal issues: for what purpose the investigative techniques could be applied, which material and formal conditions would have to be met, who would approve the implementation, whether the application would be limited only to certain persons, and how this would be achieved, how the collection of data irrelevant to the specific case would be minimized, etc. Further considerations refer to the first case of the use of hacking techniques, which are based on the use of malware.[15]

15 More about the other case of using hacking techniques and tools for search purposes, see Pisaric, 2021.

In order to create an appropriate legal framework for the use of hacking techniques to gain remote access to a protected computer system/network, it is first necessary to clearly determine the purpose of norming such a use, what would be considered by such an investigative technique, that is, what it would consist of. The meaning of the regulation would be to give a permission to the competent authorities to apply hacking techniques and tools from a distance in order to collect electronic evidence for the purposes of criminal proceedings if it concerns electronic data processing, a computer system or network that are protected by technical protection measures and which prevent or significantly make it difficult to gather evidence by implementing existing investigative measures and actions. In other words, this investigative measure may be considered as an authorized access to a protected computer or computer network for the purpose of searching or secretly monitoring communications.[16] This term is appropriate, because it is technologically neutral and broad enough, so that, in addition to the use of malware, it would also include other tools and techniques, and at the same time sufficiently specific, because it clearly indicates the nature of the activities that the competent authorities would be authorized to undertake.

Since the use of hacking techniques would represent an investigative technique with profound invasiveness, it should not be aimed at intentionally and excessively weakening technical security measures that were primarily established for the protection of user privacy. For this reason, it is necessary to clearly foresee the conditions under which such techniques can be used for the purposes of criminal proceedings. Although it could not be categorically disputed that LEA's hacking would be useful, one must not lose sight of the fact that such an authorization could have a limiting/threatening effect on certain human rights, above all the right to respect for private and family life, freedom of opinion, freedom of expression, freedom of assembly and association, etc. The initial input may be found in international legal standards concerning special investigative measures. Starting from the fact that the ECHR foresees that the limitation of the right to privacy and other relevant rights can be allowed only in certain, exceptional circumstances, the European Court has clearly established in Niemietz v. Germany that the activities of the competent authorities represent a permissible interference with these rights only on the condition that the authority of the competent authorities has a clear legal basis, that they are prescribed for the achievement of a certain

16 Different terms are used to denote this investigative technique: lawful hacking, government hacking, law enforcement hacking, network investigative techniques, remote access search and surveillance, remote computer search, remote search, etc.

legitimate goal and that it is necessary for the achievement of that goal in a democratic society.

Given that the legitimate goal of using the hacking techniques by the competent authorities is the detection and clarification of criminal acts, i.e. the collection of electronic evidence, before such an authorization would be allowed by the law, it is necessary to assess the necessity of such interference with human rights, through an assessment of subsidiarity (that whether there are less intrusive measures and actions for the achievement of the goal), effectiveness (to what extent the action would contribute to the achievement of the goal) and proportionality (to what extent the impact of the action is proportional to the achievement of the goal). In the assessment of subsidiarity, one should not lose sight of the existing investigative techniques and alternative possibilities for collecting the necessary data, which are less invasive to human rights. In addition, it is questionable how effectively this investigative technique would contribute to overcoming technical-technological obstacles to the investigation, primarily encryption.

Although examples of the use of hacking techniques by competent authorities have been known for a long time, the legal regulation in only a few countries is of recent date, so at the moment one can look with caution not only at the effectiveness of those powers, but also at the proportionality of achieving the legitimate goal (Pisarić, 2022:71). However, if despite these reservations, it is accepted that the regulation of the use of hacking techniques is necessary to overcome the problem of “Going into the dark”, the legislator could allow interference with the right to privacy and other relevant rights, by prescribing appropriate restrictions and guarantees. Whereby the legal basis for the use of hacking techniques should not be set too broadly and generally. Namely, starting from the principle of legality, the legal framework should be clear, definite and precise (UN Human Rights Council, 2013; UN General Assembly, 2016), and should contain specific provisions that would regulate hacking as an investigative technique (UN High Commissioner for Human Rights, 2014). In other words, the legislator should regulate the use of malware-hacking hacking techniques for the purposes of criminal proceedings as a special evidentiary action, and the law should establish a mechanism consisting of certain ex-ante and ex-post elements. Examples of conditions that should be met before the use, include: obtaining court approval, limiting the use of hacking techniques to more serious crimes, ensuring that the technique is appropriately targeted against specific persons/devices, limiting the duration of the measure, taking steps to ensure suitability of tools and ensuring deletion of unnecessary or third-party data. Examples of steps that should follow the use, include: notifying the person against whom the measure has been applied,

providing a means for effective monitoring of the implementation of the measure (UN Human Rights Council, 2014).

In case no explicit provisions on lawful lacking exist in the law, the use by analogy of general provisions, which were created for a different, analogous operational environment, could be brought under the “gray zone” , which due to insufficient legislative precision and clarity, would not provide a sufficient and adequate level of human rights protection. On the technical side, special attention should be paid to the acquisition of third-party hacking tools in order not to give legitimacy to the growth and cultivation of the vulnerability market. In this connection, the question of the necessity and method of disclosing vulnerability the competent authorities used is also raised. Careful and comprehensive consideration of these issues can contribute to prescribe in the most correct way the authorization of competent authorities to remotely access protected computer systems/networks/platforms and the data stored in them, or transmitted through them.

6. Conclusion

Considering certain technological tendencies, which were pointed out in the paper, within the debate on the need, measure and way of enabling state bodies to access protected electronic data processing, computer systems and networks, the lawful hacking could be of incomparable usefulness and efficiency for overcoming LEA’s obstacles in digital environment, and at the same time it represents an optimal alternative to encryption restrictions or mandatory exceptional access in terms of Going dark problem. Instead of requiring technology companies to sabotage their own protection mechanisms and thereby compromise users’ security and privacy, this alternative is based on exploiting already existing (often unintentional) vulnerabilities in the system/network. The remote access using hacker techniques may be considered as a legitimate and effective investigative technique that could contribute to overcoming the obstacles that the competent authorities face when discovering the perpetrator, conducting searches of protected computer systems and secret surveillance of electronic communications - if the competent authorities cannot determine the identity or location of the perpetrator with the help of Internet access service providers, they could access his device remotely and find the data needed for identification; if the competent authorities cannot find out the content of the suspect’s communication even through cloud computing service providers, they could gain access to the device and obtain the stored communication and intercept future conversations; if the competent authorities cannot find out the content of the encrypted data that is

stored in the device or transmitted through the network, they could gain access to the device and that data while it is decrypted, or even data needed for decryption.

Although the LEA's use hacking techniques may be a legitimate option, it still lacks the character of legality. Certain risks are immanent in the absence of a clear procedural framework - from the legal side, the potential for endangering human rights, above all the right to privacy and protection of personal data, is far higher compared to the existing investigative techniques; on the technical side, there is a risk of weakening information security. That is why it is necessary to devise an appropriate legal framework for the use of malware for the purpose of gathering evidence, while taking into account the safety and privacy of the user, especially the suspect. When considering what the legal framework governing this investigative technique should look like, it is necessary to take into account several elements. First of all, it is necessary to determine what is meant by this investigative technique, and then, considering the high degree of intrusiveness, enable its use only as an ultima ratio measure (in terms of the principle of subsidiarity), and only for the purpose of discovering and proving more serious crimes (in terms of the principle proportionality). Furthermore, it is necessary to foresee the conditions that must be met in order to be able to grant the authorization, with a clear demarcation between in situ access and remote access. In other words, the regulation governing the criminal procedure should provide for authorized access to a protected computer system/network as a special evidentiary action, and prescribe appropriate ex-ante conditions and ex-post steps.

List of references

- Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P., Rivest, R., Schiller, J., Schneier, B., Specter, M. & Weitzner D. (2015) *Keys under Doormats: Mandating insecurity by requiring government access to all data and communications*, Cambridge.
- Access Now. (2016) *A human rights response to government hacking*.
- Anstis, S. (2021) Government procurement law and hacking technology: The role of public contracting in regulating an invisible market. *Computer Law & Security Review*, *41*(1), pp. 1-16. https://doi.org/10.1016/j.clsr.2021.105536
- Application and Affidavit for Search and Seizure Warrant, In the Matter of the Search of the computers that access “Websites 1-23”.
- Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s)

of MySpace Account “Timberlinebombinfo” and Opening Messages Delivered to That Account by the Government.
- Application and Affidavit for Search Warrant, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89.
- Application for a Search Warrant, *In re* Search of Comput. that Access the Website «Bulletin Board A» Located at http://jkpos24pl2r3urlw.onion, No. 8:12MJ3 56 (D. Neb. Nov. 16, 2012).
- Application for a Search Warrant, *In re* Search of Comput. that Access the Website «Hidden Service A» Which Is Located at oqm66m6lyt6vxk7k.onion, No. 8:12MJ360 (D. Neb. Nov. 19, 2012).
- Bellovin, S., Blaze, M., Clark, S. & Landau, S. (2014) Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. *Northwestern Journal of Technology and Intellectual Property*, *12*(1), pp. 1-64.
- Carrell, N. (2002) Spying on the Mob: United States v. Scarfo - A Constitutional Analysis. *Journal of Law, Technology & Policy*, 1, pp. 193-214.
- Curran, K., Breslin, P., McLaughlin, K. &Tracey G. (2007) Hacking and Eavesdropping. In: *Cyber Warfare and Cyber Terrorism.* New York, pp. 307-317.
- Hartzog, N. (2002) The “Magic Lantern” Revealed: A Report of the FBI’s New “Key Logging” Trojan and Analysis of Its Possible Treatment in a Dynamic Legal Landscape. *Journal of Information Technology & Privacy Law*, *20* (2), pp. 287-320.
- Kerr, O., Schneier, B. (2018) Encryption Workarounds. *Georgetown Law Journal*, 106(4), pp. 989–1019.
- Mayer, J. (2018) Government Hacking. *The Yale Law Journal, 127*(3), pp. 570-662.
- Pell, S. (2016) You Can’t Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?.*North Carolina Journal of Law & Technology*, *17*(4), pp. 599 -609.
- Pisarić, M. (2016) Cross-Border Access to Data as a Way to Collect Electronic Evidence. In: Kolarić, D. (ed). *International scientific conference “Archibald Reiss Days” thematic conference proceedings of international significance* (*3*, pp. 513-520). Belgrade: Academy of Criminalistic and Police Studies.
- Pisarić, M. (2022) Communications Encryption as an Investigative Obstacle. Journal of Criminology and Criminal Law, *60* (1), pp. 61-75. https://doi.org/10.47152/rkkp.60.1.4
- Pisarić, M. (2019) *Eletronski dokazi u krivičnom postupku*. Novi Sad: Pravni fakultet u Novom Sadu.

- Pisarić, M. (2020) Enkripcija kao prepreka otkrivanju i dokazivanju krivičnih dela. *Zbornik radova pravnog fakulteta u Novom Sadu*, *54*(3), pp. 1079-1100. 10.5937/zrpfns54-26929
- Pisarić, M. (2021) Enkripcija mobilnog telefona kao prepreka otkrivanju i dokazivanju krivičnih dela – osvrt na uporedna rešenja. *Anali Pravnog fakulteta u Beogradu*, *69*(2), pp. 391-416. 10.51204/Anali_PFBU_21205A
- Response & Request to Strike Defendant's Request for Daubert Motion, U.S. v. Cottom, No. 8:13-cr-00108-JFB-TDT, at 5 (D. Neb. June 29, 2015).
- UN General Assembly (2016). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/71/373.
- UN High Commissioner for Human Rights (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*. A/HRC/27/37.
- UN Human Rights Council (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/23/4.

Višnja RANĐELOVIĆ, PhD[*]
Assistant professor
Faculty of Law, University of Kragujevac

Snežana SOKOVIĆ, PhD[**]
Full professor
Faculty of Law, University of Kragujevac

Božidar BANOVIĆ, PhD[***]
Full professor
Faculty of Security Studies, University of Belgrade

Original Scientific Article
Received: 13 March 2023
Accepted: 3 April 2023
UDK: 341.48/.49
https://doi.org/10.47152/rkkp.61.1.4

INTERNATIONAL CRIMINAL LAW AND INTERNATIONAL CRIMINAL JUSTICE OBJECTIVES AND PURPOSE OF PUNISHMENT IN INTERNATIONAL CRIMINAL LAW THEORY AND PRACTICE

Insufficient development of International Criminal Law, as well as its development under the influence of different legal systems, brought forth the lack of clear definitions of certain criminal law concepts and institutes. When considering the goals of International Criminal Law in theory they are often confused with the goals of International Criminal Justice, but also with the purpose of punishment in International Criminal Law. In that sense, the aim of the paper is, first of all, to analyse

[*] e-mail: vmilekic@jura.kg.ac.rs.

[**] e-mail: ssnezana@jura.kg.ac.rs

[***] e-mail: banovicb@fb.bg.ac.rs

theoretical understandings of the goals of International Criminal Law and Justice, as well as their definition in the acts within the field of International Criminal Law, in order to provide for the possible manner of defining and delimiting these terms. Further, the aim of the paper is to distinguish from these terms the purpose of punishment in International Criminal Law.

Key words: International Criminal Law, International Criminal Justice, the objectives, punishment, the purpose of punishment in International Criminal Law

1. Introduction

International Criminal Law as a branch of law is characterized by its still insufficient development but also by its continuous development under the influence of national criminal laws, Public International Law, and International Human Rights Law.[1] The underdevelopment of International Criminal Law is reflected both in the practice of international criminal courts, where it is not uncommon that different judges councils have different attitudes regarding the conditions or manner of application of some criminal law institutes, and also in the doctrine of International Criminal Law, where different theorists have different attitudes when defining criminal law terms, determining the elements of those terms, or classifying them.

One of the controversial issues in the International Criminal Law theory is the question of what the goals of this branch of law are. International Criminal Law theorists have rarely dealt with this issue, and among those who have tried to define the goals of International Criminal Law, taking different stands for the goal is noticeable, but also frequent permeation, or even mixing, with the goals of International Criminal Justice, or for the purpose of punishment.

It is clear that the permeation and certain coincidence between the goals of International Criminal Law and the goals of International Criminal Justice exist

1 The more intensive development of the International Criminal Law, which began during the trials before the International Military Tribunals in Nurnberg and Tokyo, was practically blocked by the outbreak of the Cold War, for this reason, the International Criminal Law in the 1990s, when trials took place before ad hoc tribunals for the former Yugoslavia and Rwanda, represented an incomplete combination of provisions in the field of International Humanitarian Law and International Human Rights Law (Adams, 2018: 750). At today's level of development, when there is a permanent International Criminal Court, it can be said that the Statute of this Court represents a kind of codification of International Criminal Law.

since the International Criminal Law, as a branch of law, is embodied in its application within International Criminal Justice. The basic goal of International Criminal Law, similarly to national criminal law, is to perform a protective function, that is, to suppress international crimes by providing protection of universally recognized goods and values from behaviour that harms or endangers them. Within the framework of International Criminal Justice, through trials for committed international crimes, the goals of International Criminal Law are realized in practice, but also some other, additional goals are achieved, such as justice, strengthening the rule of law, providing victims with closure and compensation, etc.

When it comes to the purpose of punishment, through it's prescribing and realization in practice, the goals of International Criminal Law are also achieved, thus they are related, but that does not mean that the purpose of punishment and the goals of International Criminal Law can be equalled. Namely, the goals of International Criminal Law as a branch of law are set more broadly, while the purpose of punishment is more specifically defined and related to the concept of individual-subjective responsibility and the individual as the perpetrator of an international crime.

Although there is intervening and, to some extent, overlapping between the objectives of the International Criminal Law and International Criminal Justice and the purpose of punishment in International Criminal Law, they cannot be completely identified. For this reason, the aim of this paper is to point out the existing differences between these concepts and offer a clear way to differentiate them. This could be defined as a consideration with predominant theoretical significance contributing to the development of the International Criminal Law doctrine, but its practical significance cannot be disputed, bearing in mind that it must be clear why International Criminal Justice exists, that is, which goals are strived to be achieved through trials for committed international crimes within international justice, as well as what the purpose of punishing perpetrators of international crimes by international criminal courts is.

The paper is divided in two parts, with the first part discussing the understanding of the goals of International Criminal Law and International Criminal Justice along with the purpose of punishment in both the theory and legal acts in the field of International Criminal Law, while the second part discusses these concepts in the context of their definition and understanding in international criminal courts practice.

2. International Criminal Law Objectives, International Criminal Justice Objectives and Purpose of Punishment in International Criminal Law Theory and Legal Acts

2.1. International Criminal Law Objectives

International Criminal Law as arising from the very title of this branch of law, unites the content of International and Criminal Law, therefore having both an international and criminal character. Its international character is mostly reflected in the sources of this branch of law, which are predominantly international (Cryer, et al., 2010: 16), but also in the objects of its protection and objects of its regulation. Its criminal character is reflected in the fact that International Criminal Law is by its nature criminal law, as well as that it is based on the basic concepts, principles, and national criminal law institutes. While the international character implies understanding and interpretation of the sources of international law, the criminal character requires unambiguous and precise International Criminal Law norms (Cryer, et al., 2010: 16), as well as precise basic concepts, principles, and institutes of International Criminal Law, as required by the principle of legality. When defining and prescribing the concepts, principles, and institutes of International Criminal Law, the goal of this branch of law must be kept in mind.

In the theory of national criminal law, as older one and therefore more developed than the International Criminal Law theory, there are considerations on the goals of criminal law. Although the theory of national criminal law has developed attitudes on the objectives of criminal law, they cannot simply be replicated at the level of International Criminal Law, given its international character. Despite the fact that International Criminal Law is by its nature criminal law, requirements for special definition of its goals arise from its international character. In addition to presenting the goals of International Criminal Law, the literature points out the threefold danger of making an analogy with national criminal law. *First*, the purpose of International Criminal Law is to serve numerous and very different communities, as well as the international community as a whole, which is made up of different interests. *Second*, the collective nature of international crimes, in terms of a large number of perpetrators, but also a large number of victims, significantly distinguishes these crimes from national crimes. *Third*, perpetrators of international crimes most often act in a very unstable environment, such as armed conflict, while perpetrators of national crimes most often commit these crimes in peacetime and stable environments (Sloane, 2007: 40-41).

Although, while analysing certain institutes, principles, or concepts of International Criminal Law an analogy with national criminal law cannot be accept-

able (because, among other things, the choice of specific national criminal law with which the analogy would be made, may be questioned taking in consideration numerous differences between different national legal systems), both in theory and in practice, one always starts from the views expressed in the doctrine of national criminal law. Thus, when presenting the goals of International Criminal Law, one should start from the criminal law goals, especially bearing in mind that the goals of International Criminal Law are rarely mentioned in theory, are not sufficiently analysed and explained, and are mostly associated with, or even taken for the aims of International Criminal Justice and the purpose of punishment for committed international crimes.

When considering the question of whether Criminal Law is needed at all, the theory of national criminal law points to the fact that the main reason why Criminal Law supported by criminal sanctions, should exist is deterrent or preventive in nature, because if there is a certain established application of the provisions of the Criminal Law, it has a discouraging effect on the commission of criminal offences, but also strengthens the respect for social norms (Ashworth, 1999: 16).

In the theory of Criminal Law, one can find the view that the goal of Criminal Law is to perform a protective function, that is, to suppress crime by providing protection for the most important goods and values from behaviours that injure or endanger them (Jareborg, 1995: 24-26). The performance of the protective function, as the basic goal of Criminal Law, has gained even greater importance and a more significant role at the level of International Criminal Law, given that this branch of law seeks to provide protection for the basic goods and values of universal importance for all mankind and that the suppression of international crimes is of concern to the entire international community.

The goals of this branch of law are rarely mentioned in the theory of International Criminal Law, but they all come down to the same thing - international crimes suppression. Since the International Criminal Law is by its nature and purpose Criminal Law (Stojanović, 2012: 20), the goal of this branch of law should be associated with the performance of a protective function. In that sense, the goals of International Criminal Law, which are reflected in the prevention and suppression of international crime, should be understood as an extension or expansion of the same goals of national criminal law - prevention and suppression of national crime (Bassiouni, 2014; 1, 15; Bantekas and Nash, 2007: 2). This conclusion actually makes sense because it is the issue of suppression of crimes that crosses state borders or those crimes that violate the basic values of humanity and the international legal order (Degan and Pavišić, 2005: 15), so the protective function of International Criminal Law is particularly stressed given the im-

portance of protected goods. Some authors define the prevention and suppression of international crimes as a task of International Criminal Law, but they believe that the basic task of this branch of law is still to bring justice (Zaibert, 2016: 358).

Confirmation of this understanding of the International Criminal Law goals can also be found in Paragraph 4 of the Preamble to the Statute of the permanent International Criminal Court (hereinafter “ICC”), in which the member states of the Statute confirm that the gravest criminal offences the international community is concerned about must not go unpunished and that effective prosecution of their perpetrators must be ensured by taking appropriate measures at the national level and by strengthening international cooperation. According to the views in the literature, in this way the practical goals of International Criminal Law are confirmed, *and those are the criminal prosecution and punishment of the perpetrators of the most serious crimes for which the international community as a whole is concerned about* (Triffterer, 1999: 11).

Some theorists also advocate two tasks, i.e. the role of International Criminal Law, and these are: *first*, the protection of international relations, international peace and security, that is, the international community from the so-called international crime, which represents its *protective or conservative role*, and *second*, improvement of these relations, i.e. their development in all areas aimed at improving the existing situation, which represents its *dynamic or progressive role* (Čejović, 2006: 25). In addition to performing the protective function, as the basic goal of International Criminal Law, its progressive role thus defined can be understood as an additional goal of International Criminal Law, within which one should realize that the protection of universally recognized goods promotes development and improvement in all areas.

In addition to performing the protective function, the theory of national criminal law also mentions performing the *guarantee function*, which in some way limits the protective function of Criminal Law, in the sense that citizens are also protected from Criminal Law itself, that is, from the arbitrary and unrestricted application of Criminal Law (Allen, 2007: 2; Stojanović, 2013: 24). In the future development of International Criminal Law, greater importance could be given to performing its guarantee function in terms of raising awareness and a sense of security within the international community that no person will be arbitrarily prosecuted, or that someone can be prosecuted only for the crime that, before it was been committed, was prescribed as an international crime with prescribed criminal sanction. In that way, the citizens of the world are guaranteed the realization of their basic rights and freedoms.

The literature also points to the fact that International Criminal Law is generally faced with a lack of clear definitions, which is the case, among other

things, with the goals of this branch of law, for which various English terms are used, such as objectives, aims, goals, and purposes (Heinze, 2018: 938). While the first three terms can be used in the same sense to indicate “the object to which effort or ambition is directed”, the fourth term “purpose” represents the “reason why something is done or created or the reason why something exists” (Heinze, 2018: 941). On the one hand, in that sense, the purpose of International Criminal Law is defined as the protection of basic individual and collective goods and the prevention of their violation, or the determination of the criminal responsibility of individuals for international crimes committed. On the other hand, the basic goals of International Criminal Law are international peace and security re-establishment, strengthening the protection of International Humanitarian Law, changing the culture of impunity, creating a historical record of committed crimes, satisfying the victims of crime, promoting the reconciliation process, as well as punishment of the perpetrators of international crimes (Heinze, 2018: 949). However, traditionally, the goal of Criminal Law, and, consequently, International Criminal Law is to perform its protective function.

2.2. International Criminal Justice Objectives

2.2.1. International Criminal Justice Objectives in Acts of International Criminal Law

Much more often than the goals of International Criminal Law, the goals of International Criminal Justice are defined,[2] which are contained in the preambles of the statutes, resolutions, and other acts establishing international criminal courts and tribunals. Thus, the London Agreement,[3] which established the International Military Tribunal in Nuremberg (hereinafter “NMT”), states that it is an agreement between the contracting states to *prosecute and punish the main war criminals of the European axis*, and at the beginning of the Charter[4] of this Tribunal it is underlined that Tribunal is established for the *fair and timely trial and*

2 International Criminal Justice includes international criminal institutions, like ICC, ad hoc tribunals and mixed courts, international investigation bodies and national criminal justice, that apply International Criminal Law in their joint work (Bassiouni, 2014: 909).

3 The Government of the United States of America, the Provisional Government of the French Republic, the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the Union of Soviet Socialist Republics, *London agreement*, August 8th 1945, available at: http://avalon.law.yale.edu/imt/imtchart.asp.

4 International Military Tribunal in Nuremberg, *Charter of the International Military Tribunal*, available at: http://avalon.law.yale.edu/imt/imtconst.asp.

punishment of the main war criminals of the European Axis. The Charter of the International Military Tribunal for the Far East[5] also states that the Tribunal is established for the *fair and timely trial and punishment of the main war criminals in the Far East*.

The Resolution of the Security Council No. 827[6] of 1993, which established the International Criminal Tribunal for the Former Yugoslavia (hereinafter "ICTY") first indicates that the situation in the former Yugoslavia continues to be a threat to international peace and security and that crimes should be prevented and effective measures taken to bring to justice those responsible for their execution, then the belief is expressed that the establishment of ad hoc tribunals for the prosecution of those responsible for grave violations of International Humanitarian Law will provide for the achievement of this goal and contribute to re-establishing and peacekeeping, as well as contribute to ensuring that such violence is stopped and effectively sanctioned. A further decision is cited of the establishment of an international tribunal with the *sole purpose of prosecuting those responsible for grave violations of International Humanitarian Law* committed in the territory of the former Yugoslavia starting from January 1, 1991. The first ICTY Annual Report[7] sets out the threefold purpose (objectives) of this Tribunal, arising from the Resolution No. 827: administration of justice, prevention of further crimes, and contribution to the restoration and maintenance of peace.

Member states of the Statute point out in the Preamble to the Statute of the permanent International Criminal Court, that they are aware that millions of children, women, and men have been victims of unimaginable atrocities that deeply shock the consciousness of humanity (Paragraph 2) and that such atrocities jeopardize security and welfare of the world (Paragraph 3), taking the stand that such grave crimes are no longer an internal matter of states, because they endanger the entire international community. In the literature, the third paragraph of the Preamble is presented as the International Criminal Law base, because this emerging

5 International Military Tribunal for the Far East, *Charter of the International Military Tribunal for the Far East*, available at: http://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.3_1946%20Tokyo%20Charter.pdf.

6 United Nations, Security Council, *Resolution no. 827*, from 25 May 1993, available at: http://www.icty.org/x/file/Legal%20Library/Statute/statute_827_1993_en.pdf.

7 International Tribunal for the prosecution of persons responsible for the serious violations of International humanitarian law committed in the territory of the former Yugoslavia since 1991, *Annual Report*, A/49/342 S/1994/1007, p. 11., Paragraph 11., available at: http://www.icty.org/x/file/About/Reports%20and%20Publications/AnnualReports/annual_report_1994_en.pdf.

branch of law in reality represents the Criminal Law of the community of nations, with the function of protecting the highest legal values of such a community from such grave criminal offences that jeopardize peace, security, and welfare of the world (Triffterer, 1999: 9). Furthermore, the member states of the Statute confirm that the most serious crimes of concern to the international community as a whole must not go unpunished and that effective prosecution of their perpetrators must be ensured by taking appropriate measures at the national level and strengthening international cooperation (Paragraph 4) (More: Simović-Hiber, 2012: 50-51). According to some theorists, this paragraph confirms the practical goals of International Criminal Law, namely the *prosecution and punishment of perpetrators of the most serious crimes of concern to the international community as a whole* (Triffterer, 1999: 11). Then the determination is expressed to change the current practice of impunity for perpetrators of these crimes and thus contribute to their prevention (Paragraph 5). While in previous paragraph emphasis is on criminal repression, in the fifth paragraph, in addition to repression, another goal of International Criminal Law is emphasized - *prevention*. Therefore, punishment for international crimes is in the service of their prevention, in such a way that punishment also affects those who have already committed these crimes (special prevention), but potential perpetrators also become aware that most serious crimes do not go unpunished (general prevention) (Triffterer, 1999: 12). The Member States further recall that the duty of each State is to, in accordance with its material jurisdiction, initiate criminal proceedings against persons who have committed criminal offenses governed by international instruments (Paragraph 6), that reflects the attitude that the support of national criminal legislations is required for the protection of the stated basic values. In order to achieve these goals (perpetrators of international crimes prosecution and punishment, contributing to the prevention of these crimes), the Member States of the Statute express their determination to establish an independent, permanent International Criminal Court with jurisdiction over the most serious crimes, the entire international community is concerned of (Paragraph 9).

2.2.2. International Criminal Justice Objectives in the Theory of International Criminal Law

In addition to the International Criminal Justice objectives contained in acts of International Criminal Law relating to the prosecution and punishment of in-

ternational crimes perpetrators,[8] the literature lists many other, *special objectives of International Criminal Justice*, which realization and the extent of the realization are questioned. Thus, international criminal tribunals are expected to serve great goals, such as promoting and maintaining peace and security, writing history, maintaining and promoting the rule of law, encouraging or contributing to reconciliation, and giving a voice to victims of mass crimes (Abels, 2015: 250). Some authors go a step further, supplementing and distinguishing these specific goals of International Criminal Justice from the traditional goals of criminal justice in general. On the one hand, the objectives of International Criminal Justice can be considered the *traditional* objectives of criminal justice in general, reflected in the punishment that is in the service of retribution, but also deterring perpetrators from further crime and rehabilitation, as well as deterring potential perpetrators from committing international crimes. On the other hand, there are *special objectives* that are exclusively characteristic of International Criminal Justice and that distinguish it from the national one, and they are: the rejection and stigmatization of the accused by the international community, confirmation that the international legal system is implemented and applied, ensuring satisfaction for the victims of crimes committed by the accused, efforts to end the conflict and prevent its recurrence, ending the culture of impunity, contribute to the restoration and maintenance of international peace and security, re-establishment of the rule of law, providing accurate historical data on events, reconciliation promotion in regions where international crimes have been committed (Swart, 2008: 100).

Emphasizing the fact that these are international criminal courts and tribunals, some theorists point out that they are also required to provide a panoramic picture of the context of committed international crimes, to give victims the opportunity to express their suffering and obtain compensation, to individualize punishment in order to avoid collective responsibility, to contribute to the end of conflict and stabilization, to perform the socio-pedagogical function of promoting human rights and to develop International Criminal Law. There are two problems in connection with the objectives of International Criminal Justice understood in this way, which relate to the capacity of International Criminal Justice to achieve them and the relation between the very objectives. The consequences of this are the risk of inconsistencies of court decisions, as judges may be guided by different objectives from case to case, as well as the inability to assess the performance

8 Some authors find that the interpretation of the International Criminal Law norms and their application to the case in question is the final duty of international criminal courts, based on what they decide if the defendant is guilty of committing an international crime and impose a punishment (Malekian, 2005: 676).

of international criminal courts (Damaška, 2008: 16 and further). Not only a large number of objectives, but also their diversity, lead to a “aspirations and achievements gap, tension between goals and a lack of ranking order” (Heinze, 2018: 931). These problems can be overcome either by giving up some objectives or by paying less attention to some of them. In this regard, the importance of objectives related to the aspiration of judges to shed light on the historical context of international crimes and the ambition of courts to satisfy the interests of victims should be diminished. Finally, the emphasis should be made on positive general prevention in the form of strengthening the socio-pedagogical function of promoting human rights. Therefore, the supreme task of international criminal courts would be to point out inhumane acts in verdicts, their horrors, and stigmatize their perpetrators, while the extent to which humanitarian norms will be respected and strengthened depends on the extent of their success in aforementioned. The precondition for achieving this objective is that international criminal courts represent moral authority in the societies their actions are directed to. This is sometimes very difficult to achieve, bearing in mind that the legitimacy of international criminal courts is least recognized in the environments where international crimes have been committed, and one of the reasons for this situation is the selectivity of prosecution (Damaška, 2008: 16 and further), but also an insufficient and untimely provision of information to the interested local communities by the international criminal courts, as well as an insufficient exchange of information between them. When international criminal courts make decisions, the affinities of the local communities to which those decisions apply must be taken into account, and the establishment of these courts must involve the prior democratic consent of the local community concerned (Glasius, 2012: 45-47).

The primary objectives of International Criminal Justice also stated in the doctrine are general prevention and retribution, the fight against impunity, reconciliation, and peacekeeping. In addition, two specific functions of international trials and International Criminal Justice are pointed out, namely the function of finding truth and acknowledgment, confirmation, and the function of determining responsibility. The court’s ruling, through verdicts, that the crimes were committed and the punishment of the perpetrators that follows, is an official confirmation of the committed crimes and the suffering of the victims, and prevents the falsification of history, while determining individual criminal responsibility is important for both victims and survivors. Thus, the overarching goal of International Criminal Justice is deterring from the commission of international crimes and assistance in restoring international peace and security by punishing those responsible for international crimes (D`Ascoli, 2007).

Some theorists clearly define the objectives of International Criminal Justice as prevention through intimidation; retribution through selective prosecution, which is assumed to have at least some effect of general intimidation; and providing victims with a sense of justice and closure, but consider it almost impossible to achieve these goals. The assumption that international criminal trials are likely to produce an intimidating effect and thus prevent future crimes has not yet been sufficiently investigated and confirmed, but based on the assumption of intimidation that exists in national criminal justice systems. All that remains is the symbolic of selective prosecution and its presumed impact on peace or the return to normal life in war-torn communities. At the same time, the most important objective of International Criminal Justice, which is also neglected, is to provide victims with closure and compensation (Bassiouni, 2010: 294).

Finally, the theory contains a division into three different categories of International Criminal Justice objectives. The *first category* includes those objectives similar to the classic goals of national criminal legislations: bringing perpetrators to justice, deterring them from committing international crimes in the future, and providing compensation to victims. The *second category* includes the objective of creating a historical record, a record of past events, which is very important bearing in mind that International Criminal Justice faces not only mass crimes, but also mass denials. However, the creation of a historical record is more a tool than an objective of International Criminal Justice, it is a tool that helps to understand what really happened and to decide on the criminal responsibility of the perpetrators accordingly. The *third category* includes the objectives of transitional justice, which in fact assumes that a society emerging from conflict or systematic human rights violations is learning to deal with its past and move towards a peaceful future in which human rights will be respected. These goals are, therefore, future-oriented and envisage: promoting national reconciliation, restoring the rule of law, and contributing to the restoration of peace (Galbraith, 2009: 85 and further).

From the analysed theoretical approaches it can be concluded that a division is mainly made between the *basic objectives of International Criminal Justice*, embodied in the international crimes perpetrators prosecution and punishment, and *external objectives of International Criminal Justice*, embodied in the fight against impunity, administration of justice, strengthening the rule of law, endeavouring to end the conflict and prevent its recurrence, establishing the truth for reconciliation, creation of credible historical records, providing the victims with closure and compensation, as well as the contribution to the international peacekeeping and security restoration. The literature rightly points out that such a large number of objectives and their diversity can create problems in practice, because

different judges, due to the inability to achieve all these objectives, can prioritize different objectives that lead to court decision inconsistencies. However, it is important to point out that the external objectives of International Criminal Justice are also legitimate, and that further providing the basic goals are successfully achieved, it will be easier to achieve the stated external objectives.

The legitimacy of all stated International Criminal Justice objectives is also confirmed by practice, while giving different significance to different goals. In fact, within the empirical research conducted through interviews with the staff of this Court on the effectiveness of the ICC, the respondents were supposed to give their opinion on the importance of certain objectives ICC strives to achieve. Respondents, who came from the Chambers, the Prosecutor's Office, and the Defence, were offered five objectives: fight against impunity and the prosecution of those responsible for international crimes; providing justice to victims and giving victims a voice; capacity building and national courts supplementing; conducting fair and impartial trials; contribution to peace and stability. Although most respondents considered the fight against impunity and the prosecution of those responsible for international crimes as the ICC's primary objective, their responses differed depending on whether they came from the Chambers, the Prosecution, or the Defence. Thus, respondents from the Chambers and the Prosecutions considered that the ICC's main objective was to fight against impunity and prosecute those responsible for international crimes, while the Defence respondents saw the ICC's main objectives in providing justice to victims, giving voice to the victims, national courts capacity building and supplementing (Samaria, et al., 2021: 131-132). Explaining his view that ending impunity for international crimes is a key goal of the ICC, one Chambers respondent pointed out that the *ultimate goal* is to encourage national judiciaries to do their job while the ICC should set an example and give the reason how this would be done. In doing so, the ICC in the long run will no longer have to exist (Samaria, et al., 2021: 133). According to those interviewed, differing views on what the ICC's main objective is can lead to conflict situations in the Court's functioning, due to different views on what the Court should prioritize and how it should be reflected in the Court's daily activities (Samaria, et al., 2021: 135). However, it should be borne in mind that despite the different views on the basic objectives of the ICC, that is a logical consequence of the fact that the respondents belong to different bodies within this Court, all of them are participants in the same procedure, and their synergistic action enables a number of different objectives achievement.

After analysing the above provisions of the acts international criminal courts and tribunals are established on and different views expressed in the liter-

ature, we believe that the content of the preambles of the statutes of international criminal courts, resolutions, and other establishing acts of these courts, called the *objective* or *purpose* of their establishment and that is criminal prosecution and punishment of persons responsible for international criminal offenses, we can understand as a *basic task of international criminal courts*, that is, the *task of International Criminal Justice* (Similarly: Samaria, et al., 2021: 127). This approach becomes clearer if paralleled with the task of national criminal justice, which is to prosecute perpetrators of criminal acts (which is within the competence of the public prosecutor) and trial of the perpetrators of criminal acts, i.e. clarification and resolving criminal matters (which is within the competence of the criminal court) (Bejatović, 2014: 128, 157-158).

By performing this task, international criminal courts contribute to the achievement of the *objectives of International Criminal Justice*, which are broadly set and aimed at the international community as a whole, and can be defined as: fighting impunity, administration of justice, strengthening the rule of law, endeavours to conflict ending and preventing its re-occurrence, establishing truth for reconciliation, providing victims with closure and compensation, as well as contributing to the restoration of international security and peacekeeping.

In terms of historical record making (More: Wilson, 2011), which is often cited as the International Criminal Justice objective, the argument is on the part of those authors who believe that it is more a *tool* than an *objective*, because it assists the understanding of what really happened and to decide upon it on criminal liability of perpetrators.

2.3. Purpose of Punishment in International Criminal Law

Since the purpose of punishment in theory is often confused with the objectives of International Criminal Law and International Criminal Justice, which is logical since the purpose of punishment does not exist in itself, it is important to determine what is meant by the purpose of punishment in International Criminal Law in order to distinguish these terms because, as mentioned earlier, they cannot be equalled. The difference between the objectives of International Criminal Law and International Criminal Justice, on the one hand, and the purpose of punishment on the other, is already visible at the level of concepts. As pointed out earlier, the term “objective” should indicate “the object to which effort or ambition is directed”, while the term “purpose” represents “the reason why something is done or created or the reason why something exists” (Heinze, 2018: 941). Starting from such notions of objective and purpose it can be concluded that the

objective of the International Criminal Law is directed towards certain objects, that is, goods and values that are protected by International Criminal Law due to their universal significance. The objective of International Criminal Justice is aimed at those entities that have been injured or threatened by international crimes, such as victims (their protection and compensation), peace and security (their re-establishment), rule of law (its strengthening), etc. Finally, the purpose of punishment in International Criminal Law can be determined as the reason why penalties are prescribed and imposed for perpetrators of international crimes.

From this definition of the stated terms, it is clear that, despite certain permeation and coincidence, they cannot be equated. On the one hand, the objectives of International Criminal Law are broadly set, as providing protection to universally recognized goods and values, accordingly the International Criminal Law in itself already acts as a general preventive measure. On the other hand, the purpose of punishment is more specifically defined and is related to the concept of individual-subjective responsibility of individuals as perpetrators of international crimes, whose punishment at the individual level shows that International Criminal Law is applied. In this way, through the application of International Criminal Law by International Criminal Courts, i.e. through criminal prosecution and trial of international crimes perpetrators, all previously mentioned objectives of International Criminal Justice are achieved.

3. Purpose of Punishment in International Criminal Courts Practice

It is interesting to point out that no act within the International Criminal Law determines the purpose of punishment, since the statutes of international criminal courts and tribunals do not contain such provisions, unlike national criminal laws which, as a rule, prescribe the purpose of punishment and determine it as part of certain Criminal Law institutes.[9] However, although the purpose of punishment is prescribed in national criminal law, it cannot simply be replicated

9 For example, in the Republic of Serbia, the purpose of punishment is prescribed by the provision of Art. 42. Of Criminal Code as: 1. preventing the perpetrator from committing criminal offenses and influencing him/her not to commit criminal offenses in the future; 2. influencing others not to commit crimes; 3. expressing social condemnation for a crime, strengthening morals and strengthening the obligation to respect the law. It is interesting to point that in Art. 24 of the ICTY Statute stipulates that when determining a prison sentence, the trial chamber will have in mind the general practice of imposing prison sentences in the courts of the former Yugoslavia. According to the Criminal Code of Serbia, the basic criteria for sentencing are the prescribed punishment for a certain criminal offense, the purpose of punishment and mitigating and aggravating circumstances (Article 54, Paragraph 1 of the Criminal Code), so the ICTY should take into account the purpose of punishment.

at the level of International Criminal Law, primarily because of the difference in nature and characteristics among ordinary and international crimes. Namely, international crimes are characterized by mass violence, i.e. the existence of a large number of international crimes perpetrators and the existence of a large number of victims of those crimes. In practice, this leads to the selective prosecution of only the most responsible perpetrators of the most serious international crimes, which calls into question the idea of retribution and deterrence, as the basic purposes of punishment in International Criminal Law. The idea of retribution implies that the perpetrators "get what they deserve", and if the criminal prosecution is selective - this idea has not been consistently implemented. Also, deterrence cannot fulfil its function, if all perpetrators of (international) crimes are not prosecuted and punished (Maculan and Alicia, 2020: 145-146).

As the purpose of punishment is not prescribed in International Criminal Law, it is left to court practice to determine the purpose of punishment in each specific case, and the views of court practice are very different because they range from branding the defendant to rehabilitation as a way of special prevention achieving. It is notable that the case law does not deal with the issues of the International Criminal Law objectives or the International Criminal Justice objectives as theoretical issues, but with the issues of the purpose of punishment, which is logical since the Chambers deal with concrete perpetrators of international crimes that should be punished in accordance with the principle of individual subjective responsibility.

Since the verdicts of the International Military Tribunals in Nuremberg and Tokyo did not contain explanations, the purpose of punishment was not discussed either (Banović and Bejatović, 2011: 211-212). The ICTY and ICTR judgments state different purposes of punishment (Comprehensive: Keller, 2001), but two are highlighted as basic: retribution and deterrence. In the *"Čelebići"* case, the ICTY Appeals Chamber pointed out that the cases dealt with by the ICTY differed significantly from those normally dealt with by national courts, primarily because of the gravity of the crimes being tried, as they constituted grave violations of International Humanitarian Law and the two main purposes of punishment for these crimes are deterrence and retribution.[10] However, in the opinion of the ICTY Appeals Chamber in the *Aleksovski* case, deterrence is an important factor in sentencing international crimes, but should not be given too much importance, given that retribution is an equally important factor and should be understood as a desire to express the international community's dismay at the crimes committed,

10 Judgment, *"Čelebići"* (IT-96-21-A), Appeals Chamber, 20 February 2001,§ 806; Judgement, *Furundžija* (IT-95-17/1-T), Trial Chamber, 10 December 1998, § 288.

since the ICTY's punishment should make the international community's condemnation of the crimes committed obvious and show that the international community is unwilling to tolerate grave violations of International Humanitarian Law and human rights.[11]

In addition to retribution and deterrence, as the basic purposes of punishment for committed international crimes, some chambers cited reprimanding and stigmatization of defendants as purposes of punishment. For example, in the *Erdemović* case, the ICTY Trial Chamber took the stand that reprimanding and public stigmatization by the international community, which thus expressed its disgust at the committed crimes and branded their perpetrators, represented the key purpose of imprisonment for crimes against humanity.[12]

Some judgments already made by the Chambers of the permanent International Criminal Court mention retribution, special and general prevention as purposes of punishment. In the *Katanga* case, in the Decision on punishment in accordance with Article 76 of the Statute[13] and in the first instance Judgment in the *Bemba* case,[14] retribution, and prevention are emphasized as the two main purposes of punishment. Allegedly, according to the views of the trial chambers the role of punishment is twofold: on one hand, it is the expression of social condemnation of the committed crime and the perpetrator, recognizing in this manner injuries and sufferings inflicted on victims, and, on the other hand, deterrence aimed at deterring those who plan to commit a similar crime from that intent. In the first instance Judgment in the *Al Mahdi* case,[15] the Trial Chamber starts from the view that, according to the Preamble to the ICC Statute, retribution and deterrence are two primary purposes of punishment. At the same time, retribution should not be understood as revenge against the accused, but condemnation of the international community for the committed crimes, through which, by imposing a proportional punishment, the injury committed to the victims is also recognized and peace and reconciliation are promoted. With regard to deterrence, the Trial Chamber considers that the sentence should be adequate in the sense that it should discourage the convicted person from re-offending (special prevention) as

11 Judgment, *Aleksovski* (IT-95-14/1-A), Appeals Chamber, 24 March 2000, § 185.

12 Judgment, *Erdemović* (IT-96-22-T), Appeals Chamber, 29 November 1996, § 65.

13 Decision on Sentence pursuant to Article 76 of the Statute, *Katanga* (ICC-01/04-01/07), Trial Chamber II, 23 May 2014, § 38.

14 Decision on Sentence Pursuant to Article 76 of the Statute, *Bemba Gombo* (ICC- 01/05-01/08), Trial Chamber III, 21 June 2016, §§ 10-11.

15 Judgment and Sentence, *Al Mahdi* (ICC-01/12-01/15), Trial Chamber VIII, 27 September 2016,§§ 66-67.

well as ensure that those in consideration of committing similar offenses are deterred from doing so (general prevention).

One gets the impression that deterrence and prevention in the mentioned decisions, are sometimes used as synonyms that are also recognized by the doctrine. Neither practitioners nor theorists of International Law often recognize or acknowledge the difference between deterrence and prevention, where deterrence is based on the hedonistic calculation of the individual weighing the potential benefits against costs, while prevention involves governmental and local programs, policies, and initiatives aimed at reducing the risk factors of criminal behaviour and the victimization rate, strengthening the application of law and the administration of justice, and changing the perception that leads to the commission of criminal offenses (Schense, 2017: 25-26). Although the stated ICC judgments use the term deterrence, the term prevention is sometimes also used as a synonym for deterrence, which again indicates the International Criminal Law underdevelopment, as a branch of law.

As *deterrence* has been singled out as one of the most important purposes of punishment for committed international crimes, the question is raised as to what extent it is possible to achieve the effect of deterrence by punishment by international criminal courts and tribunals.

Searching for the answer to the aforementioned question (See more: Rothe and Victoria, 2013), one study came to the conclusion that similar to the case of national courts, it is difficult to “assess” the deterrent effect of international criminal courts and tribunals. On the one hand, in some cases, despite the fact that criminal proceedings have been initiated, or even passing the verdict by these tribunals and courts, conflict and international crimes commission have continued in the countries of origin of the defendants (for example, in case of former Yugoslavia and DR Congo). On the other hand, in the countries where the conflict calmed down, there were some other circumstances that led to the calming of the conflict (for example in Darfur), so it is not possible to determine the correlation with certainty between initiating trial or passing the conviction by international criminal courts and tribunals and conflict calming (See more: Schense and Carter, 2017: 430-434). While it cannot be claimed with certainty that the existence and operation of international criminal tribunals have absolutely no effect on the settlement of conflicts, it would not be right to claim or expect these tribunals to directly and deliberately contribute to international peace and security (Mégret, 2018: 847).

In cases with the young defendants, the Chambers justifiably took into account another purpose of punishment - rehabilitation. In the *Furundžija* case

before the ICTY, the defendant was 24 years old at the time of the critical events and 29 at the time of the first instance verdict, so the Trial Chamber also calls for rehabilitation as a purpose of punishment given the defendant's age - the fact that he is young.16 In the *Erdemović* case before the ICTY, the defendant was 23 years old at the time of the critical events and 25 at the time of the first instance decision, so the Trial Chamber considered the fact of his young age as a *mitigating circumstance* when sentencing,17 clarifying that his young age and character indicated the possibility of his change and that he should be given another chance to start his life from the beginning after his release, while he is still young enough to do so.18 However, due to the specific nature of the crimes within the ICTY's jurisdiction, the Chamber considered that, regardless of the age of the accused, there was no possibility of considering any rehabilitative purpose of punishment, but rehabilitation as a purpose of punishment must give way to stigmatizing the gravest violation of International Humanitarian Law in order to prevent the reoccurrence. This does not mean that prison treatment alone cannot have rehabilitation as a goal.19 The attitude against rehabilitation as a purpose of punishment is confirmed by Appeals Chamber in the "*Čelebići*" case before the ICTY, which points out that although national legislations and certain international and regional human rights instruments envisage the possibility that courts deciding on the sentence must take into consideration before all the rehabilitation, the rehabilitation itself cannot have the dominant role in the decision-making process of the ICTY Chambers, taking into account the fact that ICTY cases differ from those dealt with by national courts, primarily regarding the seriousness of the crimes being tried.20

Regarding the *purpose of punishment*, the analysis of the decisions of international criminal courts shows that retribution and deterrence stand out as the main purposes of punishment. The greatest importance is attached to retribution, having in mind the gravity of the crimes that are being tried before these courts. Also, the argument is on the side of those authors who believe that the emphasis should be on positive general prevention. Namely, in the international courts judgments, it is important to point out the inhumanity and terrible consequences of committing international crimes, all with the aim of strengthening and

16 Judgment*, Furundžija* (IT-95-17/1-T), Trial Chamber, 10 December 1998,§ 291.

17 Judgment, *Erdemović* (IT-96-22-T), Trial Chamber, 29 November 1996,§§ 47-48.

18 Sentencing Judgement, *Erdemović* (IT-96-22-Tbis), Trial Chamber, 5 March 1998,§ 16.

19 Judgment, *Erdemović* (IT-96-22-T), Trial Chamber, 29 November 1996,§ 66.

20 Judgment, *"Čelebići" (*IT-96-21-A), Trial Chamber, 20 February 2001, § 806.

enhancement of respect for those norms that provide protection to basic goods and values of humanity, since adoption and compliance with such norms before all impact the non-commission of international crimes.

4. Conclusion

The fact is that International Criminal Law is a still developing branch of law, that this development is influenced by main legal systems with all their diversity, but also different requirements within the international community, international relations development, and the practical needs of International Criminal Justice caused that in the theory of International Criminal Law there is often interference, but also different attitudes on the basic objectives of International Criminal Law, the objectives of International Criminal Justice and the purpose of punishment in International Criminal Law.

Although at first glance theoretical topic, defining and delimiting the objectives of International Criminal Law and the objectives of International Criminal Justice is of great practical importance in directing the future development of International Criminal Law as a branch of law, as well as in directing the work of international criminal courts and their impact on national criminal justice.

Understanding the objective in general as “an object towards which effort or ambition is directed to”, it can be concluded that the basic objective of International Criminal Law is to perform a protective function, i.e. providing protection for the most important goods and values, universally accepted by the entire international community from endangering behavior. Thus the defined objective of International Criminal Law should be understood as an extension of the basic objective of national criminal law, emphasizing that protective function performance gains even greater importance at the international level, having in mind the importance and value of protected goods, i.e. their universality. In the future development of International Criminal Law, within the framework of its progressive role, greater importance should be given to the International Criminal Law guarantee function realization, aimed at providing respect for the rights and freedoms of all members of the international community.

The International Criminal Law objectives derive from International Criminal Law acts, especially from the international criminal courts statutes, where international criminal acts are defined as behaviors that violate or endanger universally recognized goods and values. However, these goals would remain a “dead letter” if there were no international criminal courts that apply the rules contained in International Criminal Law acts, allowing these goals to be achieved.

This is made possible by the fact that perpetrators of international crimes are prosecuted by the international criminal courts which is the basic task of these courts. By performing their basic task, international criminal courts not only contribute to the achievement of the basic goals of International Criminal Law, but also to the achievement of the of International Criminal Justice objectives, which are broader and focused on the international community as a whole, exemplified in the fight against impunity, administration of justice, strengthening the rule of law, endeavours to end the conflict and prevent its recurrence, establishing the truth for reconciliation, providing victims with closure and compensations, as well as contributing to the re-establishment and maintenance of international peace and security.

The objectives of International and National Criminal Justice also largely coincide, such as: the administration of justice, strengthening the rule of law, and providing victims with closure and compensation. However, International Criminal Justice, due to its jurisdiction over international crimes, characterized by the fact that they are most often committed during an armed conflict, has its own objectives, namely: the fight against impunity, efforts to end the conflict and prevent its recurrence, establishing the truth for reconciliation, as well as contributing to the restoration and maintenance of international peace and security. Due to such numerous and diverse objectives, there may be inconsistencies in the case law due to different views regarding goals that should be given priority. Nevertheless, the successful realization of the basic task of International Criminal Justice - criminal prosecution and punishment of perpetrators of international crimes, enables the easier realization of all external goals of International Criminal Justice.

While in theory the issues of the goals of International Criminal Law and International Criminal Justice are considered, the case law, logically, deals with the question of the purpose of punishment, considering that it is related to the concept of individual-subjective responsibility of specific perpetrators of international crimes. In order to distinguish the objectives of International Criminal Law and International Criminal Justice from the purpose of punishment in International Criminal Law it is first necessary to point out the difference that already exists at the level of concepts, where the purpose is now understood as “the reason why something was done or created or the reason because something exists.” In that sense, the purpose of punishment in International Criminal Law, embodied primarily in retribution and deterrence, is more specifically set, directly in connection with the concept of individual-subjective responsibility and individuals as perpetrators of international crimes. Punishing perpetrators of international crimes

international community expresses condemnation for committing such serious crimes, which should also influence the deterrence from their further commission, and in this manner, the purpose of punishment is achieved in the International Criminal Law. Its realization practically achieves the objectives of International Criminal Law as well as the objectives of International Criminal Justice, because only in that way - by punishing the perpetrators of international crimes, it is clear that International Criminal Law is applied and that International Criminal Justice really fulfils its mission.

Literature

- Abels, D., (2015). The Objectives of International Punishment. In: R. Mulgrew & D. Abels, (eds.) *Research Handbook on the International Penal System*. Cheltenham; Northampton: Elgar Publishers, pp. 250-273.
- Adams, A. (2018) The Legacy of the International Criminal Tribunals for the Former Yugoslavia and Rwanda and Their Contribution to the Crime of Rape. *The European Journal of International Law,* 29(3), pp. 749-769. https://doi.org/10.1093/ejil/chy043
- Allen, M. (2007) *Textbook on Criminal Law.* 9th ed. Oxford: Oxford Univeristy Press.
- Ashworth, A. (1999) *Principles of Criminal Law.* 3rd ed. Oxford: Oxford University Press.
- Banović, B. & Bejatović, S. (2011) *Basics of International Criminal Law.* 1st ed. Kragujevac: Faculty of Law University of Kragujevac.
- Bantekas, I. & Nash, S. (2007) *International Criminal Law.* 3rd ed. London; New York: Routledge Cavendish.
- Bassiouni, C. (2010) Perspectives on International Criminal Justice. *Virginia Journal of International Law,* 50(269), pp. 269-300.
- Bassiouni, C. (2014) *Introduction to International Criminal Law.* 2nd ed. Leiden; Boston: Martinus Nijhoff Publishers.
- Bejatović, S. (2014) *Law of Criminal Procedure.* 3rd ed. Kragujevac: Faculty of Law University of Kragujevac.
- Cryer, R., Friman, H., Robinson, D. & Wilmshurst, E. (2010) *An Introduction to International Criminal Law and Procedure.* 2nd ed. Cambridge: Cambridge University Press.
- Čejović, B. (2006) *International Criminal Law.* 1st ed. Belgrade: Dosije.
- D`Ascoli, S. (2007) International Sentencing and the Undefined Purposes of International Criminal Justice'. *Jura Gentium.*

- Damaška, M. (2008) Real Objectives of the International Criminal Justice. *Croatian Yearbook of Criminal Law and Practice,* Volume 15.
- Damaška, M. (2008) Rights and Objectives of International Criminal Justice. *Croatian Yearbook of Criminal Law and Practice,* Volume 15.
- Degan, V. & Pavišić, B. (2005) *International Criminal Law.* Rijeka: Faculty of Law, Rijeka.
- Galbraith, J. (2009) The pace of International criminal justice. *Michigan Law Review,* 31(79), pp. 79-143.
- Glasius, M. (2012) Do International Criminal Courts Require Democratic Legitimacy?. *The European Journal of International Law,* 23(43), pp. 43-66. https://doi.org/10.1093/ejil/chr104
- Heinze, A. (2018) Bridge over Troubled Water – A Semantic Approach to Purposes and Goals in International Criminal Justice. *International Criminal Law Review,* 18(6), pp. 929-957. https://doi.org/10.1163/15718123-01806006
- Jareborg, N. (1995) What Kind of Criminal Law Do We Want?. *Scandinavian Studies in Law. In: Beware of Punishment: On the Utility and Futility of Criminal Law,* Volume 14, pp. 19-.
- Keller, A. (2001) Punishment for Violations of International Criminal Law: An Analysis of Sentencing at the ICTY and ICTR. *Indiana International and Comparative Law Review,* Issue 12, pp. 53-74.
- Maculan, E. & Alicia, G. G. (2020) The rationale and purposes of criminal law and punishment in transitional contexts. *Oxford Journal of Legal Studies ,* 40(1), pp. 132-157. https://doi.org/10.1093/ojls/gqz033
- Malekian, F. (2005) Emasculating the Philosophy of the International Criminal Justice in the Iraqi Special Tribunal. *Cornell International Law Journal,* 38(3), pp. 673-723.
- Mégret, F. (2018) International criminal justice as a peace project. *European Journal of International Law,* 29(3), pp. 835-858. https://doi.org/10.1093/ejil/chy057
- Rothe, D. & Victoria, C. (2013) The International Criminal Court: A Pipe Dream to End Impunity?. *International Criminal Law Review,* 13(1), pp. 191-209. https://doi.org/10.1163/15718123-01301006
- Samaria, M., Holá, B. & Dirkzwager, A. (2021) Reimagining the ICC: Exploring Practitioners` Perspectives on the Effectiveness of the International Criminal Court. *International Criminal Law Review, 21*, pp. 126-153. https://doi.org/10.1163/15718123-bja10039

- Schense, J. (2017) Assessing Deterrence and the Implications for the International Criminal Court. In: J. Schense & L. Carter, eds. *Two Steps Forward, One Step Back: The Deterrent Effect of International Criminal Tribunals.* Brussels: Torkel Opsahl Academic EPublisher, pp. 13-62.
- Schense, J. & Carter, L. (2017) Findings and Recommendations. In: J. Schense & L. Carter, eds. *Two Steps Forward, One Step Back: The Deterrent Effect of International Criminal Court.* Brussels: Torkel Opsahl Academic EPublisher, pp. 427-458.
- Simović-Hiber, I. (2012) Modeli evropskog krivičnog prava i statuta međunarodnih krivičnih tribunala u realizaciji ideje nadnacionalnog krivičnog prava. *Journal of Criminology and Criminal Law,* 50(3), pp. 37-60.
- Sloane, R. (2007) The Expressive Capacity of International Punishment: The Limits of the National Law Analogy and the Potential of International Criminal Law. *Stanford Journal of International Law,* 43(39), pp. 39-94.
- Stojanović, Z. (2012) *International Criminal Law.* 7th ed. Belgrade: Pravna knjiga.
- Stojanović, Z. (2013) *Criminal Law - General Part.* 20th ed. Belgrade: Faculty of Law, University of Belgrade.
- Swart, B. (2008) Damaška and the Faces of International Criminal Justice. *Journal of International Criminal Justice,* 6(1), pp. 87-114. https://doi.org/10.1093/jicj/mqm082
- Triffterer, O. (1999) *Commentary on the Rome Statute of the International Criminal Court.* 1st ed. Baden-Baden: Nomos Verlagsgesellschaft.
- Wilson, R. A. (2011) *Writing history in international criminal trials.* 1st ed. Cambridge: Cambridge University Press.
- Zaibert, L. (2016) Rules, Games, and the Axiological Foundations of (International) Criminal Law. *International Criminal Law Review,* 16(2), pp. 346-360. https://doi.org/10.1163/15718123-01602007

Legal acts:

- The Government of the United States of America, the Provisional Government of the French Republic, the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the Union of Soviet Socialist Republics, *London agreement*, August 8th 1945, available at: http://avalon.law.yale.edu/imt/imtchart.asp.
- International Military Tribunal in Nuremberg, *Charter of the International Military Tribunal*, available at: http://avalon.law.yale.edu/imt/imtconst.asp.

- International Military Tribunal for the Far East, *Charter of the International Military Tribunal for the Far East*, available at:
- http://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.3_1946%20Tokyo%20Charter.pdf.
- United Nations, Security Council, *Resolution no. 827*, from 25 May 1993, available at: http://www.icty.org/x/file/Legal%20Library/Statute/statute_827_1993_en.pdf.
  - International Tribunal for the prosecution of persons responsible for the serious violations of International humanitarian law committed in the territory of the former Yugoslavia since 1991, *Annual Report*, A/49/342 S/1994/1007, p. 11., Paragraph 11., available at: http://www.icty.org/x/file/About/Reports%20and%20Publications/AnnualReports/annual_report_1994_en.pdf.

Courts` decisions:

- Decision on Sentence pursuant to Article 76 of the Statute, *Katanga* (ICC-01/04-01/07), Trial Chamber II, 23 May 2014.
- Decision on Sentence Pursuant to Article 76 of the Statute, *Bemba Gombo* (ICC- 01/05-01/08), Trial Chamber III, 21 June 2016.
- Judgment, *Aleksovski* (IT-95-14/1-A), Appeals Chamber, 24 March 2000.
- Judgment, *Erdemović* (IT-96-22-T), Appeals Chamber, 29 November 1996.
- Judgment and Sentence, *Al Mahdi* (ICC-01/12-01/15), Trial Chamber VIII, 27 September 2016.
- Judgment*, Furundžija* (IT-95-17/1-T), Trial Chamber, 10 December 1998.
- Judgment, *“Čelebići”* (IT-96-21-A), Appeals Chamber, 20 February 2001.
- Sentencing Judgement, *Erdemović* (IT-96-22-Tbis), Trial Chamber, 5 March 1998.

Aleksandra ILIĆ, PhD*
Associate Professor,
Faculty of Security Studies
University of Belgrade

Review paper
Received: 19 March
Accepted: 20 April
UDK: 343.848
343.24(497.11)
https://doi.org/10.47152/rkkp.61.1.5

THE ANALYSIS OF SOME PROBLEMS IN ACHIEVING THE REHABILITATION PURPOSE OF PUNISHMENT

In this work the author deals with contemporary problems in achieving the rehabilitation aim as a dominant purpose of prison sentence execution in majority of countries today. Rehabilitation is one of the major principle in treating of persons who are convicted to prison sentence and consists of numerous rules set in some international documents as well as in national legislations. In work is given an overview of the historical development of the rehabilitation model both in global and domestic level as well as modern approaches in realization of rehabilitation expectations. The author further analysis some retributive tendentions in modern legislation. One of the problem is the trend of imposing a life sentence which is particularly problematic in case of absence the possibility of parole for certain convicts. That form of life sentence is prescribed in Criminal Code of Republic Serbia, so the author considers the sustaintability of that provision, especially in the context of European Court of Human Rights's decisions.

Keywords: rehabilitation, prisons, punishment, retribution, life sentence

* e-mail: alex.mag.ilic@gmail.com

1. Introduction

Nowadays, the modern penalty system faces with a lot of challenges. There are a lot of questions that are waiting for the answers and a lot of dillemmas in the context of the future direction in the development of the sanctioning for criminal acts. If we analyze the global tendencies toward the treatment of crime perpetuators in the past few decades, it can be seen the two main conclusions. First one means introduction of restorative justice principle which is in line with so called alternative treatment in sanctioning for criminal acts as well as alternative solutions in conducting the criminal proceeding (plea bargaining for example).

Second one is completely on the opposite side and is close connected to the retribution concept and severe sanctioning in some cases ie. for some criminal acts, usually because of the nature of criminal act or fact who is a victim. That tendency means use of prison to a great manner, both as a criminal sanction and as a measure for guaranting the presence of the accused person during the criminal procedure ie. as a detention. In both situations, main goal of the states with high percentage of deprivation of liberty is keeping society safe. But the question is wheather fulfilling the prisons brings the achievement of safety. In most countries, the evidence is clear that there is no satisfaction in gaining the primary goal of incarceration. In the United States (US), two in three (68%) of people released from prison are rearrested within three years of release. In England and Wales, two in three (66%) of young people and nearly half of adults leaving prison will commit another crime within a year[1].

Beside the fact of uneffectiveness of imprisonment in many countries, to reduce crime rate there are tendency around the world of introducing the retributive elements in sanctioning for crimes without profound analysis of effectiveness of such approach usually because retributive oriented public expects that kind of measures and at the same time politicians strive to fulfill those expectations. In connection with that, integral part of the political story about the necessity of sharp confrontation to the different forms of criminal activity is indicating on „seriousness“ of the criminality issue (Ilić, 2017: 183). On the other hand very often the legislator doesn’t show consistency which means that by nature similar criminal acts don’t receive the similar treatment. Special treatment is especially present in dealing with convicts for sexual assaults (particularly when children

1 World Economic Forum, Prisons are failing. It’s time to find an alternative. Available at: https://www.weforum.org/agenda/2019/01/prisons-are-failing-time-for-alternative-sparkinside/ page accessed 01.03.2023.

are victims) and also when it comes to supression of extremism and terrorism, which is part of a popular counter-terrorism framework. In this second case, it is not important whether individuals are accused or convicted and there are no differences between mere extremist on the one side and terrorist activities on the other side, everything „deserves“ special treatment from prison staff.

Other problem which arises from retributive legislative solutions is the possibility of achieving the rehabilitation effect, having in mind that principle of rehabilitation still dominates, at least on paper, in treatment of convicts in many countries around the world and, more important, which is part of the most significant international documents in this field. Traditionally, in penology literature under criticism were put short term (to six months or one year longest) and long term (ten years or more)[2] prison sentences because neither both of them are capable in a large manner, to fulfill the expectations of rehabilitation. But without doubt, life sentence, to the greatest extent, calls into the question the possibility of achieving the rehabilitation. The longiness of life sentence, even with possibility of parole, creates strong limitations which unable positive results in rehabilitation. However, life sentence with the possibility of parole gives some kind of hope to convict that one day could be realesed. In that sense, life sentence without parole is strong negation of rehabilitation and shouldn’t be part of the legal provisions. Unfortunately, there are some countries, like Serbia, which decided to ignore that fact referring to the higher interest of protecting society from the most dangerous attacks on its values.

2. General notes on Rehabilitation concept

The rehabilitation as purpose of punishment is one of the basic principle of modern imprisonment execution system, together with individualisation in execution of imprisonment and humanity approach in treatment of convicts (Ignjatović, 2019: 181). The aim of rehabilitation model is to reform or resocialize criminals to conventional, law-abiding values (Hagan, 2008: 107). More detailed, rehabilitation is a process, intervention or programme to enable indviduals to overcome previous difficulties linked to their offending so that they can become law-abiding and useful members of the wider community (Burnett, 2008: 243). A broad array of programs have been used to bring about such changes, including

2 Recommendation Rec(2003)23 of the Committee of Ministers to member states on the management by prison administrations of life sentence and other long-term prisoners defines a long-term prisoner as one who is serving a prison sentence or sentences totalling five years or more.

education, job training, psychological and medical treatment, prison ministries, and recreation (Pollock, 2006: 158).

In domestic literature, Milutinović pointed that rehabilitation means procedures of personality socialization of persons who have been already socialized, but in a negative manner. That is about persons who had gone through the socialization process, but that process negatively ended and which led to the conflict with the ruling system of social norms and rules of conduct (1977: 81). On the other hand, Atanacković argued that negative socialization is not possible, if person doesn't respect social norms and social values and doesn't behave according to the norms and values, there is no room for discussion on socialization at all. In other words, it is necessary to make distinction between „formed personality“ and „socialized personality“ and further formed personality could be socialized and nonsocialized. As a consequence of those distinction, between rehabilitation of formed and nonformed personality there are some differences, primarly in the ways of gaining the goals of elimination the criminal behaviour in future and preparation for integration in social life (Atanacković, 1988: 130, 131).

The history of rehabilitation doesn't start with modern prison system, a long time it is stated as a goal of corrections. The first systematic prison system, which was created in frame of Classical system – the Cellular Isolation system, within its two separate models: solitary confinement system and system of silence, was based on redemption, moral transformation and strong discipline. At that time, the accent was still on retribution as a purpose of punishment. In the mid-1800s, the idea of individualized treatment began to take hold and not all offenders could be expected to respond to prison programs in the same way. Captain Maconochie's mark system, which tied inmate behavior to privilages and early release, and Sir Walter Crofton's Irish system of phased release were early attempts to encourage rehabilitation by offering incentives for good behaviour (Pollock, 2006: 159). The both of the systems were called Combine Progressive system which idea was to combine retributive and rehabilitative elements at the same time. Even it might seemed to be the best solution for the inmates, the practical experiences weren't so good which influenced the abandoning of it and direction to the system which is based just on one principle. Everything was leading to the rehabilitation model.

The United Nations Standard Minimal Rules for the Treatment of Prisoners (hereinafter: SMRTP) (the Nelson Mandela Rules)[3], prescribes that all prisoners shall be treated with the respect due to their inherent dignity and value as human

3 Standard Minimum Rules for the Treatment of Prisoners Standard Minimum Rules], RES/663 C (1957) and RES/2076 (1977) Adopted by the First United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held at Geneva in 1955, and approved by the Economic and Social Council by its resolution 663 C (XXIV) of 31 July 1957 and 2076 (LXII) of 13 May 1977,

beings. Further, no prisoner shall be subjected to, and all prisoners shall be protected from, torture and other cruel, inhuman or degrading treatment or punishment, for which no circumstances whatsoever may be invoked as a justification (Rule 1). The SMRTP contains minimal conditions that should be provided in dealing with convicts and they are imagined to be, in every country which accepts them, as a ground for building the imprisonment execution system (Ignjatović, 2019: 181).

Among basic principles of Rules of general aplications, which contains SMRTP, in the context of rehabilitation, it should be emphasized the following rule: „The purposes of a sentence of imprisonment or similar measures deprivative of a person's liberty are primarily to protect society against crime and to reduce recidivism. Those purposes can be achieved only if the period of imprisonment is used to ensure, so far as possible, the reintegration of such persons into society upon release so that they can lead a law-abiding and self-supporting life. To this end, prison administrations and other competent authorities should offer education, vocational training and work, as well as other forms of assistance that are appropriate and available, including those of a remedial, moral, spiritual, social and health- and sports-based nature. All such programmes, activities and services should be delivered in line with the individual treatment needs of prisoners“ (Rule 4).

Beside SMRTP, since Republic of Serbia is part of the Council of Europe, another very important document which considers the position of convicts and other prisoners and, in connection with that, prescribes rules which oblige states, is European Prison Rules (hereinafter: EPR). In the Recommendation Rec(2006)2 of the Committee of Ministers to member states on the EPR[4] it is stressed that the enforcement of custodial sentences and the treatment of prisoners necessitate taking account of the requirements of safety, security and discipline while also ensuring prison conditions which do not infringe human dignity and which offer meaningful occupational activities and treatment programmes to inmates, thus preparing them for their reintegration into society. As it is obvious from the previous sentence, the most important outcome which should derive from the prisoners residence in prisons is reintegration into society.

The rehabilitation concept is present in Serbian legislative on execution of criminal sanction more than seven decades. At the beginning it was developed within the legislative of former Yugoslavia. The first regulation which contained

available at: https://www.unodc.org/documents/justice-and-prison-reform/Nelson_Mandela_Rules-E-ebook.pdf, page accessed on 15.02.2023.

4 Recommendation Rec(2006)2 of the Committee of Ministers to member states on the European Prison Rules (Adopted by the Committee of Ministers on 11 January 2006 at the 952nd meeting of the Ministers'Deputies).

progressive principles like idea of re-education, together with ideas of joint sentence serving and classification of convicts was Temporary Instruction on Penal Execution[5] (Atanacković, 1988: 262). According to the Instruction, the aim of the sentence is not only punishing the guilty, but also re-educating the condemned in spirit of loyalty to the motherland, work discipline and honorable attitude towards state and social relations, training the convicted for the conditions of common life and the consolidation of those features of his character that will keep him from further committing the crime (Knežić, 2017: 122). For the first time in 1948, the matter of execution of criminal sanction was regulated in law. That year it was brought the Law on Penal Execution[6] which developed in a greater manner the modern principles of penal execution but three years later another law in this matter was brought: Law on Execution of Penal Sentence, Security Measures and Educational-Corrective Measures[7], which achieved another step further in modernization of criminal sanction execution and in developing the idea of rehabilitation of convicts as a main purpose of execution of criminal sanctions. In that law it was mentioned for the first time the establishment of special service for post-penal assistance (Atanacković, 1988: 263, 264). Big step in further modernization of Yugoslavian and Serbian penitentiary system represented the Law on Execution of Criminal Sanctions from 1961[8] which introduced many new institutions and modern solutions as part of a realization the SMRP rules that Yugoslavia accepted. With no doubt the principle of rehabilitation dominated in penitentiary system of Yugoslavia and Serbia in that time. Kupčević-Mlađenović noted that rehabilitation priciple had programmatic character and the whole action in treatment of convicts were subordinated to its realization (1972: 180, 181). After the constutional reform in 1974 Serbia, as all other republics of former Yugoslavia, got its own Law on Execution of Criminal Sanction[9]. The purpose of penal sentence execution was achievement of rehabilitation and social rehabilitation of the crime perpetrator. More precisely it was prescribed that the purpose was preparation of convict for living and working in accordance with law and fulfillment the duties of man and citizen of socialist self-governing community (Atanacković, 1988: 275). That Law was replaced exactly two decades later with the homonymous

5 Temporary Instruction on Penal Execution (Cab. no.1199 from 27.september 1945).

6 Law on Penal Execution (Official Gazette FNRJ, no. 92/48).

7 Law on Execution of Penal Sentence, Security Measures and Educational-Corrective Measures (Official Gazette FNRJ, no. 47/51).

8 Law on Execution of Criminal Sanctions (Official Gazette FNRJ, no. 24/61).

9 Law on Execution of Criminal Sanctions (Official Gazette SRS, no. 26/77, 50/84, 46/86 and 16/87).

law[10] which didn't determine at all the purpose of penal sentence execution and it was replaced in 2005 with new Law on Execution of Criminal Sanctions[11] that contained the provision on purpose of criminal sanction execution[12]. That provision was unpropriate and was criticized in theory, as well as Amendments from 2009[13] that brought some changes in precribed purpose[14] but not enough (Ignjatović, 2018: 174). Finally, the current Law on Execution of Criminal Sanctions[15] contains the purpose of penal sentence execution as adoption of socially acceptable values through appropriate treatment programs during the execution of the sentence in order to facilitate inclusion in living conditions after the execution of the sentence so that the convicts would not commit crimes in the future. In such prescribed purpose it can be seen the importance of special prevention (Ilić, 2022: 128).

3. Criticism of Rehabilitation model

Despite dominant legislation solutions, both international and domestic, part of the theory is not so convinced that prisons are places where convicts could change themselves in a proper manner. Particular problem is the fact that some offenders are not able to be changed or they don't want to be changed. Finally, some of them are completely well socialized and there is no need for prison treatment of any kind. On the other hand successfull rehabilitation is connected to well organized prison system which further means qualifed prison staff, who are present in optimal number and treat each convict as a specific individual with unique combination of characteristics, provided all facilities important for realization of rehabilitation program and many other things. All of it is very hard to complish in many countries. In relation with that, some scholars put into the question the possibility of the imprisonment execution system to achieve the requirement of rehabilitation, especially because of the constant high rate of reo-

10 Law on Execution of Criminal Sanctions (Official Gazette RS, nos. 16/97 and 34/01).

11 Law on Execution of Criminal Sanctions (Official Gazette RS, nos. 85/2005 and 72/2009).

12 The precribed purpose was „implementation of legally binding and enforceable court decisions, protection of society from criminal acts and separation of perpetrators of crime from the social environment for the purpose of their treatment, care and training to take care of their own needs after the execution of the sanction“.

13 Law on Amendments and Additions to the Law on Execution of Criminal Sanctions (Official Gazette RS, no. 72/2009).

14 New purpose after amendments was: „suppression of acts that injure or threaten people and basic social values“.

15 Law on Execution of Criminal Sanctions (Official Gazette RS, nos. 55/14 and 35/19).

ffending in many countries. That is highly connected to the crime statistics which is one of the most important tool for the practitioners as well as scholars in analyzing the effectiveness of modern penalty system.

The truth is that crime statistics have been a part of the discourse of many states for over 200 years, but the advance of statistical methods permits the formulation of concepts and strategies that allow direct relations between penal strategy and the population. Earlier generations used statistics to map the responses of normatively defined groups to punishment; today one talks of "high-rate offenders," "career criminals," and other categories defined by the distribution itself. Rather than simply extending the capacity of the system to rehabilitate or control crime, actuarial classification has come increasingly to define the correctional enterprise itself (Feeley, Simon, 1992: 453, 454).

It seems that today the most important question is what is the evidence that prison treatment works. MacKenzie pointed out that strategies for reducing crime should be based on scientific evidence which refers to the need to use scientific evidence to make informed decisions about correctional policy (2006: 20). In other words, the dominant discourse on this is about evidence-based corrections. In the context of such approach much of the debate about rehabilitation hinges on whether treatment programs are effective in reducing recidivism (Cullen, 2012: 95, 96). In academic debate everything started with Robert Martinson's systematic assessment of the program evaluation literature from 1945 to 1967 whose account of the results was famously called the „nothing works“ essay because he concluded that „With few and isolated exceptions, the rehabilitative efforts that have been reported so far have had no appreciable effect on recidivism“ (1974: 25, according to: Cullen, 2012: 96). Cullen claims that Martinson's study had a crucial influence in reframing the debate over rehabilitation because it consolidated complex arguments into a single, simple issue: if treatment programs do not work, then how can anyone continue to support rehabilitation as the guiding theory of corrections? Uttering the slogan that „nothing works“ was a powerful way to avoid broader policy concerns and to silence all argument. Both liberals and conservatives used Martinson's work in this way (Cullen, 2012: 96). But even Martinson modified his opinion, concluding after further research that treatment programs could be beneficial, neutral, or detrimential to recidivism, depending on the conditions under which they were provided (Martinson, 1979, according to Pollock, 2006: 160,161).

Some authors stated that by the last decade of the twentieth century, rehabilitation had renewed credibility calling it as a „new rehabilitationism“. This new approach is more focused on offending behaviour than on the whole person, and

the objective is to prevent reoffending with a view to increasing community security, rather than to rehabilitate an individual as an end in itself (Rayner, Robinson, 2005, according to Burnett, 2008: 243). One of the reason for such approach is raising of the demand for security in every aspect of the society - the securitization of the society which is further connected to the concept of risk society (Beck, 2011) ie. the tendency of construction the risks in modern society as globalized and common thing for majority of people and necessity to establish full control over them – culture of control (Garland, 2001). Under the rationale of „offender responsibilization“ contemporary penal regimes have undertaken widespread surveillance practices to assist rehabilitative capacities and reform risky forms of conduct (Monagham, 2012: 6).

One of the best example of two mentioned concepts: risk society and culture of control in the context of a „new rehabilitationism“ is in the case of terrorism and extremism. In many countries, within the „new era“ narrative on terrorism as a global threat, there are efforts as a part of the counter-terrorism policy, for introducing the specific way of dealing with persons not just convicted but also suspected for the acts of terrorism as well as extremism. That kind of hysteria over necessity of completely different and exclusive treatment of individuals, somehow connected to terrorism and extremism, is not in a compliance with the traditional and still worldwide present system of imprisonment execution where accent is on individual approach in treatment of convicts, which takes into account personal ability of change.

It can be said that the main reason of such narrative is about the otherness of terrorism and its perceived hostility to the „essence“ of liberal democracy that justifies increasingly vigilant measures taken by courts, police and correctional agencies. Perceived threats are to „our very way of life“ – however vague the threats may be – are understood in the most immediate and all-encompassing danger to collective security, and thus deserving of exemplary punishment (Monaghan, 2012: 8). Further, when governments justify the need to segregate and/or isolate inmates who have been charged or convicted of terrorism related offences from other prisoners, they commonly raise concerns about their correctional facilities becoming „breeding grounds“ or „universities“ for terrorism (Useem, Clayton, 2009: 562 according to: Jones, 2014: 74). The truth is that much of the discussion so far has been one-sided because an underlying assumption is that prisons are thought to be schools for terrorism (Jones, 2014: 75).

Second question which arises from the context of increasing incarceration of prisoners prosecuted for acts related to terrorism, what is the prison administration’s ability to adapt and provide solutions to this growing and specific form

of crime (Chantraine, Scheer, 2021: 261). In other words „what works“ for the terrorism? What kind of rehabilitation program? Is really necessary for the states to develop specific approach in dealing with terrorism or any other crime? These are questions that urgently need answers.

Particular requests for different treatment of terrorism is in line with so called „new penology“ as a new decision-making analysis used in the penal sector, which is essentially concerned with the identification, classification, categorization and management of delinquents and prisoners on the basis of their membership of a more-or-less ‘at risk’ group (Feeley, Simon, 1992 according to Cliquennois, 2013: 468). According to the two American theorists, Malcolm Feeley and Jonathan Simon, the new penological era inaugurates an amalgam of actuarial policies aimed at the effective control of selected risk groups and efficient system management, rather than embracing the traditional objectives of rehabilitation or punishment of individual offenders (Cheliotis, 2006: 313, 314). Also, some authors in Serbia analyzed the penal problemacy from the perspective of new penology. According to Soković, the task of the new penology is to manage crime, not to rehabilitate criminals, to “normalize” criminality, not to eliminate it. The goal is to maintain the integrity of the social control system, which does not include additional external ones social goals such as the elimination of crime and the reintegration of criminals. Hence, the new penology is less interested in the diagnosis and treatment of the individual criminal, and more in the identification, classification and management of criminal groups classified according to the degree of risk of their behavior in relative to the normed order. The new penology has no aspirations to rehabilitate and reintegrate, yet to manage the risk of future criminal behavior, primarily through various modalities of arresting the offender (Soković, 2011: 219).

If we put the problemacy of rehabilitation and its un(success) in reducing recidivism and generally control over crime in society in the phrame of different criminological perspectives, that was a moment when positivist theoretical approach in analyzing criminal phenomenon came into the crisis, surrounded together with different neoclassical tendencies on the one side and critical criminology on the other side. Focus of the positivists were always on individual or\and social characteristics that contribute to the commitment of the crime and in connection with that to the process of reducing those factors. From that point of view, treatment of convicts especially in prison facilities is the best way in achieving the goal of elimination causes of crime and final result – rehabilitation of the offenders and their successful reintegration in society.

The opposite theoretical approaches have different attitude on the importance of rehabilitation. Neoclassicists don't deal with causes of crime but practical questions of daily crime fight ie. „what works“ (Hagan, 1990 according to: Ignjatović, 2019: 65), which is in line with Martinson's conclusion of failure of rehabilitation model. These theorists have sparked an interest in the abandonment of treatment and rehabilitation and in a return to the classical punishment model and incapacitation of offenders, because simply criminals in jail can no longer victimize. On the other side, while the neoclassicists argue that less theory and more action is needed, they at times ignore the fact the basic theoretical underpinnings of their own theories are rooted in assumptions of eighteenth-century hedonism, utilitarianism, and free will (Hagan, 2008: 104). Beccaria, Bentham and other classicists gave precious contributions to the construction of modern criminal law but some of their findings aren't appropriate for apply in dealing with offenders today.

Also opposite then positivistic approach, the critical criminologists distinguish other problems connected to rehabilitation model. Despite the fact that critical criminology consists of different theoretical approaches (labeling theory, radical theory, new critical theory, feminist theory...) some of the characteristics are common and it can be summarized to following: crime is a label attached to behaviour, usually that of the less powerful in society and in connection with that the process of labeling is under the control of more powerful groups. Further, the conflict model rather than the consensus model explains the criminalisation process and crime is often understood as a rational response to inequitable conditions in capitalistic societies (Hagan, 2008: 176). Critical criminologists, but especially those who are part of the new critical approach, are responsible for some kind of diversification in treatment of offenders in generally. For example, Hulsman is one of the originator of the idea of restorative justice and his efforts were directed toward reduction of the prison sentences number and its replacement with a fine and also for introduction the model of "diversification of criminal procedure" which today dominates in modern criminal procedure due to its efficiancy (Ignjatović, 2019: 84). During the 1970, Hulsman conducted research on sentencing which brought him to the conclusion that is almost impossible from the criminal law system to be derived the legitimate sentence, taking into account the way that system functions (Hulsman, Bernat de Celis, 2010: 17). Hulsman is also well known for his request directed to reduction of crime number in positive legislatives because there are number of examples where some behaviour could be erased from criminal law without introducing any other mechanism to replace it (Hulsman, Bernat de Celis, 2010: 61) which means the decriminalization that is

the least popular process in contemporary's dynamic of criminal law which are dominantly retributive oriented. It should be mentioned another scandinavian author – Thomas Mathiesen who gave important contribution to the humanization of criminal politics in his country (Norway) and generally in Scandinavia but his influence was broader for sure. He worked within the framework of the Norwegian Association for Penal Reform which one of the basic principle was participation of current and former prisoners in work of that organization. That principle was important for the three reasons: permeation of theory and practise on prisons, maintenance of knowledge on prisons and prison life and increasing knowledge on prison life (Matisen, 2019: 54, 55).

Retributive philosophy is essential part of the advocating for severe sentences like death penalty or life sentence and which are negation of the rehabilitation requirement in treatment of offenders. That is connected to penal populism. Policies are populist if they are advanced to win votes without much regard for their effects. Penal populists allow the electoral advantage of a policy to take precedence over its penal effectiveness (Roberts et al., 2003: 5 according to: Hamilton, 2022: 3). John Pratt delivers a dire prognosis of the future of criminal justice under populism: „the fundamental expectations of and limits to punishment in democratic society are likely to crumble still further – in the name of a security and sense of well-being and safety that becomes ever more elusive and distant“ (2020: 294, according to Hamilton, 2022: 7).

In further text it will be considered the practical and theoretical problemacy of life sentence which is still very popular way of sanctioning the offenders around the globe. Special attention will be paid to the situation in Republic of Serbia because of the life sentence without possibility of parole, which was introduced into the Criminal Code (hereinafter: CC) in 2019, in relation to certain categories of offenders.

4. Life sentence and Rehabilitation – global overview

Life-sentence prisoner can be defined as one serving a sentence of life imprisonment. Life-sentence prisoners are those sentenced indeterminately as a rule because life sentence does not usually mean that a prisoners spends his or her whole life in prison (Solomon, 2008: 153). Legal solutions on life-sentence differ from country to country. In most countries who have been prescribed life sentence, possibility of parole is guaranteed as a right of life-sentence prisoners after some period of time spending in prison. Also some countries have several variations of life sentence. For example, in England and Wales life sentence prisoners

include those who have received mandatory, discretionary and automatic life sentences, and those who are detained under indeterminate public protection sentences (Solomon, 2008: 153).

The most recent worldwide data on life imprisonment, published in 2019, estimated that in 2014 there were 479,000 people serving a formal life sentence. However, this excludes informal life sentences – where the sentence imposed may not be called life imprisonment but may result in the person being detained in prison for life. Furthermore, data available at the national level point to an upward trend in the number of life sentences imposed and also increased punitiveness in length, conditions and the types of offences that can attract a life sentence (Global prison trends 2022: 17).

Life-sentences are part of all the national jurisdictions with the exception of Portugal, where the maximum sentence that can be imposed is 25 years. Nevertheless, even in Portugal, there are complaints of effective life sentences: be they due to a sentencing scheme of consecutive, aggregated sentences which in effect far exceed the 25 years stipulated by law, to the super-imposition of more sentences incurred while serving the original sentence, or the age of the prisoner at the time of the conviction, many are those who see themselves as serving a “life sentence” (even if they, theoretically, can be appealed, reduced and do admit leaves) (Maculan et al., 2013: 45).

In Recommendation Rec(2003)23 of the Committee of Ministers to member states on the management by prison administrations of life sentence and other long-term prisoner[16] (hereinafter: Recommendation Rec(2003)23 of the Committee of Ministers), it is emphasized that the abolition of the death penalty in member states has resulted in an increase in the use of life sentences and also in many countries, in the number and length of long-term sentences, which contribute to prison overcrowding and may impair the effective and human management of prisoners.

In general there are no special plans and life prisoners are treated in the same way as other prisoners. As for other inmates, their sentence plans should be drawn up individually, but due to a lack of resources, the possibility to participate in work, training, education or cultural activities is often limited also for lifers. In England and Wales, for example, the difficulty in enrolling in courses that would help to demonstrate risk diminution (due to lack of resources to provide

16 Recommendation Rec(2003)23 of the Committee of Ministers to member states on the management by prison administrations of life sentence and other long-term prisoners (Adopted by the Committee of Ministers on 9 October 2003 at the 855th meeting of the Ministers’ Deputies).

such courses in overcrowded prisons), makes release all the harder to achieve (Maculan et al., 2013: 46).

The sentencing framework in generally has become much tougher in recent years in many countries. In England and Wales for example, a whole life tariff should be applied to adults over the age of 21 who commit multiple murders; a terrorist murder; a murder of a child following abduction or involving sexual conduct; and a murder where the offender has been previously convicted of murder (Solomon, 2008: 154). Similar, US approach in sentencing stands out in the Western worlds which was observed by Michael Torny as „practices that many Americans endorse – capital punishment, three-strikes laws, prison sentence measured in decades or lifetimes – are as unthinkable in other Western countries as are lynchings and public torture in America“ (Barkan, 2009: 518).

Life sentence in its substance is problematic in the context of realization of the rehabilitation principle. Even if the concrete legislation prescribes possibility of parole, main question is wheather the achievement of rehabilitation is realistic aim in cases of life sentence convicts. If the answer is no, the further question is how to legitimize the existence of that sentence in majority of legislation taking into account that the principle of rehabilitation is one of the main pillars of the modern imprisonment execution system.

Recommendation Rec(2003)23 of the Committee of Ministers also stresses that the enforcement of custodial sentences requires striking a balance between the objectives of ensuring security, good order and discipline in penal institutions, on the one hand, and providing prisoners with decent living conditions, active regimes and constructive preparations for release, on the other. It is also stressed that legislation and practice concerning the management of life sentence and other long-term prisoners should comply with the requirements embodied in the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: Convention)[17] and the case-law of the organs entrusted with its application.

4. 1. Life sentence and Rehabilitation in Republic of Serbia

Adequately arranged criminal justice system implies that all its elements are connected and coordinated. This concretely means that the three basic se-

17 Law on Ratification of the European Convention for the Protection of Human Rights and Fundamental Freedoms with Additional Protocols, with amendments and additions, Official Gazette of the Serbia and Montenegro - International Agreements 9/03, 5/05 and 7/05 - correction and Official Gazette of the RS - International Agreements 12/10 and 10/15.

gments of criminal justice system: material, procedural and executive, must start from the same principles, that is, serve the same goals. For the purposes of this work, in particular should be emphasized the importance of the connection between the substantive legal provisions contained in the CC concerning the general purpose of punishment and the corresponding provisions contained primarily in the Law on Execution of Criminal Sanctions[18] (hereinafter: LECS) as the basic law in the field of execution.

Law on Amendments and Additions to the CC in 2019[19] (hereinafter: LAA-CC/2019) brought some important changes in criminal law approach to certain crimes and certain perpetuators. These changes, among others, include: life sentence was introduced, the right to parole was revoked for perpetrators of certain crimes, stricter punishment was prescribed in case of reoffending, and the range of crimes for which a conditional sentence can be imposed was narrowed (Ilić, 2019: 123,124). We will here put the accent on the life sentence, especially life sentence without the possibility of parole, and generally new provisions concerning parole, all in the context of rehabilitation unachievability in Republic of Serbia.

The Article 44a prescribes that in exceptional cases, life sentence may be pronounced along with imprisonment, for the most severe criminal offences and the most severe forms of severe criminal offences. In connection with that, a life sentence cannot be pronounced to a person who, at the time of commission of a criminal offence is less than twenty-one years of age and also life sentence cannot be pronounced in cases when the law sets forth that a penalty can be mitigated (Article 56, paragraph 1, item 1 of CC) or when there is basis for acquittal. The fact is that life sentence replaced imprisonment for 30 to 40 years, which was once introduced as a substitute for the death penalty. If we just take into account that simple fact, without further analyses it is obvious that with this new solutions Serbian CC makes steps toward strengthening the retributive approach in punishment of criminals. It is with no doubt clear that the legislator cared to satisfy very quickly the aspirations of one part of the public without entering into the question the justification of this penalty and the replacement of the existing solution (Stojanović, 2020: 233).

The nature of the new CC provisions is also evidenced by the addition of Article 42, more precisely, the introduction of another goal that should be achieved through the purpose of punishment. Among existing purposes: to prevent an offender from committing criminal offences and deter them from future commission of

18 Law on Execution of Criminal Sanctions (Official Gazette RS, Nos. 55/14 and 35/19).

19 The Law on Amendments and Additions to the Criminal Code (Official Gazette RS, No. 35/19).

criminal offences (special prevention); to deter others from commission of criminal offences (general prevention) and to express social condemnation of the criminal offence, enhance moral strength and reinforce the obligation to respect the law, the new item 4 of the Article 42, introduced achieving fairness and proportionality between the committed act and the severity of the criminal sanction, as a new purpose of punishment. This new purpose of punishment is clear manifestation of retributivism which takes into account only the past fact – commited crime and seeks for proportionate sentencing, which is basically act of retaliation.

The main reason for the introduction of life sentence is the legislator's determination to prescribe it for the most serious crimes against life and limb and crimes against sexual freedom in cases where the death of a child, minor, pregnant woman or helpless person occurred as a result of the crime[20]. For the mentioned crimes the court may not release on parole a convicted person[21] ie. Republic of Serbia introduced life sentence without possibility of parole.

Such a solution caused a stormy reaction from the Serbian's professional public, which indicated, and still indicates, the unsustainability of such a solution from the point of view of Serbia's membership in the Council of Europe and, in accordance with that, the obligations assumed by signing the Convention which also refers to the obligation to respect decisions of the European Court of Human Rights (hereinafter: ECHR). According to the concept of the reintegration of convicts into society, which dominates the penological practice of European countries from the 1980s to the present day, and is also expressed in Council of Europe documents, prison isolation of a person sentenced to death must not be the sole purpose of applying the prison (life) sentence - not only because the personality of the convicted person and his danger to society change over time, but also because of problems in the management of the prison system in which convicts who are not motivated to respect the prison regime are held for a long time, and because of their advanced age they have increasing problems with health and special medical and social needs (the so-called phenomenon of "grey" prisons) (Mrvić-Petrović, 2022: 408). One of the most important question that arises is there any point in sending a convicted person to reception department, to make a plan of dealing with him and what would motivate him as to change the strictest regime (with which execution usually begins) to a milder one (Ignjatović, 2019: 133).

20 Reasoning of the Proposal of LAACC/2019. These are following crimes: Aggravated murder (Article 114, paragraph 1, item 9), Rape (Article 178, paragraph 4), Sexual intercourse with a helpless person (179, paragraph 3), Sexual intercourse with a child (Article 180, paragraph 3) and Sexual intercourse by abuse of position (Article 181, paragraph 5).

21 Article 46, paragraph 5 of the CC.

On the other hand, some authors point to the fact that even in case of life sentence with possibility of parole, some convicts don't really have a chance for release, because of the nature of provisions in the field of criminal sanction execution which means that there a slightly chance for positive report on parole from prison authorities in case of person convicted for severe crime with life sentence (Ilić, 2019: 167).

Imposing a life sentence on an adult perpetrator of a criminal offense is not prohibited by any provision of the Convention. This sentence can come under the "impact" of Article 3 of the Convention which relates to prohibition of torture if the convicted person has no prospect of being released, which means that there is no mechanism in national law to review the conviction of life sentence with the aim of its modification *in melius*, early or conditional release. In order to meet the standard set by Article 3 of the Convention, it is necessary, according to the position expressed in the judgment of *Vinter and Others v. the United Kingdom*[22], that the person convicted to life sentence has the right to know at the beginning of the life sentence what and under which conditions he must do in order his release to be considered, as well as to know when his sentence will be reviewed or when he can request it. If the domestic law does not provide any mechanism or possibility to review the life sentence, the non-compliance of that sentence with Article 3 of the Convention on this basis appears already at the moment of its imposition, and not during its serving (Ilić, 2019: 132). Review of a sentence is necessary because the grounds for detention (punishment, deterrence, public protection and rehabilitation) may change in relevance during lengthy imprisonment. It is obvious that provision on life sentence in CC is not compatible with the practice of the ECHR, i.e. that it represents a violation of Article 3 of the Convention, because our law does not know any other effective mechanism that would allow the review of this sentence after a certain period of time (Ćorović, 2021: 85).

Without fixing a time limit, the ECHR noted the support in European domestic and international law for a guaranteed review within the first 25 years of a sentence[23]. In one of the recent decision, Chamber judgment in the case of *Bancsók and László Magyar (no. 2) v. Hungary*[24] the ECHR held, unanimously, that there had been: a violation of Article 3 of the Convention. The case concerned the imposition of life sentences with eligibility for release on parole only after 40

22 ECHR *Vinter and Others v. the United Kingdom*, Nos. 66069/09, 130/10 and 3896/10, 09.07.2013.

23 Human Right Law Centre, available at: https://www.hrlc.org.au/human-rights-case-summaries/2017/8/23/european-court-of-human-rights-rules-that-irreducible-life-sentences-violate-human-dignity, page accessed on 15.03.2023

24 ECHR *Bancsók and László Magyar (no. 2) v. Hungary*, nos. 52374/15 and 53364/15, 28.01.2022.

years of imprisonment. The ECHR found that such sentences did not, in effect, offer any real prospect of release, and were thus not compatible with the Convention. The question is whether the solution in CC (convicted to life sentence, after twenty-seven years served in prison acquires the right to seek parole (Article 46, paragraph 2, alinea 1)) is in accordance with the ECHR practice. Turanjanin considers that Serbian provision is in line with the ECHR standards because the legal term of 27 years begins to run from the day of deprivation of liberty, while the stated standard of 25 years refers to the period after the sentencing of life imprisonment (2021: 22), taking into account that ECHR in its judgments “primarily calls for the possibility of re-examination after the sentencing to life imprisonment”, while in CC, the time spent in detention, in serving a measure of prohibition to leave the apartment, as well as any other deprivation of liberty in relation to a criminal offence shall be credited to the pronounced prison sentence, fine and community service (Article 63, paragraph 1). On the other hand, Ćorović thinks that mentioned provision has to be novelled by explicitly mentioning life imprisonment, which represents a special punishment in our law, as to avoid any dilemmas in that sense (2021: 84).

For the end of this section, it is interesed to be mentioned the case of Columbia in the context of life sentence. The Constitutional Court of Columbia ruled in September 2021 that the recent introduction of life sentence (with a possibility of review after 25 years) for the crimes of rape and sexual abuse of children was unconstitutional. The Court found that life sentences are contrary to human dignity, threaten the guarantee of resocialisation of convicted persons and are a setback that risks dehumanising the penal system[25](Global Prison Trends 2022: 17).

5. Conclusion

As a conclusion, the main question which arises from the previous analysis is what will happen with rehabilitation, what is the future of the concept that was imagined to be the best way of dealing with prison convicts in modern society. Does it have chance to survive? Further from this point, if rehabilitation is meant to go into the history, what will replace it.

Retribution elements are some how always present in most countries, their advocates are waiting for an ideal moment to start with the promotion of its superiority. It is so easy to reach for a retribution solution when public is not satisfied with crime state. There is always something which disturbs public, some sort

25 Corte Constitucional, Communicado 33, Septiembre 2 de 2021, Sentencia C-294/21.

of crime which has pottential to cause strong emotional reaction of the public. But illusion is that there is some kind of magical wand for solving the problem of crime. Like Dirkhaim said, crime is normal social fact, always present in societies, from the appereance of human kind. The only trick is to sustain the crime on the acceptable level, not to allow it to exceed the optimal level that corresponds to the characteristics of a certain society.

Announcing of introduction the more severe sanctions or some new harder forms of existing crimes or completely new crimes is one of the best way for gaining the political points. The fact is that the modern society is functioning basically on the ground of retributive philosophy and demand for sharper sanctioning of the offenders.

But the truth is that only with prevention efforts things will become better. If we successed to prevent crime, we are in good direction. One of the way of prevention is to influence the perpetrator not to reoffend and the best solution for gaining that goal is removing the conditions that lead to the commission of the previous crime. From that point of view, rehabilitation is still the best option we have.

References

- Atanacković, D. (1988) *Penologija*. Beograd: Naučna knjiga;
- Barkan, S. E. (2009) *Criminology: a sociological understanding, Fourth edition.* Upper Saddle River: Pearson Prentice Hall.
- Bek, U. (2011) Svetsko rizično društvo: u potrazi za izgubljenom sigurnošću (Weltrisikogesellschaft: Auf der Suche nach der verlorenen Sicherheit, Suhrkamp Verlag, Frankfurt am Main, 2007, translator: Glišović Lj.). Novi Sad: Akademska knjiga.
- Burnett, R. (2008) Rehabilitation, in: Y. Jewkes & J. Bennet (eds.) *Dictionary of Prisons and Punishment*. Willan Publishing: Devon, pp. 243-245.
- Chantraine, G. & Scheer, D. (2021) Performing the enemy? No-risk logic and the assessment of prisoners in “radicalization assessment units” in French prisons. *Punishment & Society*, 23(2), pp. 260-280. https://doi.org/10.1177/1462474520952147
- Cheliotis, L. (2006) How Iron Is the Iron Cage of New Penology? The Role of Human Agency in the Implementation of Criminal Justice Policy. *Punishment & Society*, 8(3), 313-340. https://doi.org/10.1177/1462474506064700
- Cullen, F.T. (2012) Taking rehabilitation seriously. *Punishment & Society*, 14(1), pp. 94-114. https://doi.org/10.1177/1462474510385973.

- Ćorović, E. (2021) Doživotni zatvor i uslovni otpust u krivičnom pravu srbije: neka pitanja i dileme. *Revija za kriminologiju i krivično pravo*, (1), pp. 69-92. https://doi: 10.47152/rkkp.59.1.1
- Feeley, M.M. & Simon, J. (1992) The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications. *Criminology*, *30*(4), pp. 449-474. https://doi.org/10.1111/j.1745-9125.1992.tb01112.x
- Garland, D. (2001) The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: The University of Chicago Press.
- Global Prison Trends (2022) *Penal Reform International*. Thailand Institute of Justice.
- Hagan, F.E. (2008) Introducing to Criminology: Theories, Methods, and Criminal Behaviour, 6th Edition. Los Angeles: Sage.
- Hamilton, C. (2022) Radical right populism and the sociology of punishment: Towards a research agenda. *Punishment & Society,* pp. 1-21, : https://doi.org/10.1177/14624745221114802.
- Hulsman L., Bernat de Celis, J. (2010) *Izgubljene kazne – krivični sistem pod znakom pitanja* (prevod dela: *Peines Perdues – Le Système Pénal en Question,* Paris, 1982, prevodilac: Đokić, I.), Edicija CRIMEN. Beograd: Pravni fakultet Univerziteta u Beogradu.
- Human Right Law Centre, available at: https://www.hrlc.org.au/human-rights-case-summaries/2017/8/23/european-court-of-human-rights-rules-that-irreducible-life-sentences-violate-human-dignity, page accessed on 15.03.2023
- Ilić, A. (2017) *Mediji i kriminalitet-kriminološki aspekti*, doctoral dissertation defensed at the Faculty of Law University of Belgrade.
- Ilić, A. (2022) Komentar Zakona o izvršenju krivičnih sankcija. Beograd: Službeni glasnik.
- Ilić, G. (2019) Marginalije o kazni doživotnog zatvora, uslovnom otpustu i ljudskim pravima. In: Đ. Ignjatović (ed.), *Kaznena reakcija u Srbiji IX deo*. Beograd: Pravni fakultet Univerziteta u Beogradu, pp. 123-142.
- Ignjatović, Đ. (2019) *Kriminologija*. Beograd: Pravni fakultet Univerziteta u Beogradu.
- Ignjatović, Đ. (2019) Kazna doživotnog zatvora – razlozi uvođenja i osvrt na rešenja u poslednjoj noveli krivičnog zakonika. In: S. Bejatović (ur.), *Izmene u krivičnom zakondavstvu i statusu nosilaca pravosudnih funkcija i adekvatnost državne reakcije na kriminalitet (međunarodni pravni standardi i stanje u Srbiji)*, LIX redovno godišnje savetovanje Srpskog udruženja za krivičnopravnu teoriju i praksu, Zlatibor - Beograd, pp.119-141.

- Ilić, V. (2019) (Ne)pomirljivost kazne doživotnog zatvora i ljudskih prava. *CRIMEN*, 10(2), pp. 156–173; 10.5937/crimen1902156I
- Jones, C. R. (2014) Are prisons really schools for terrorism? Challenging the rhetoric on prison radicalization. *Punishment & Society,16*(1), 74-103, https://doi.org/10.1177/1462474513506482
- Knežić, B. (2017) *Obrazovanje osuđenika: Način da se bude slobodan*. Beograd: Institut za kriminološka i sociološka istraživanja;
- MacKenzie, D. (2006). Evidence-Based Corrections. In: *What Works in Corrections:Reducing the Criminal Activities of Offenders and Deliquents* (Cambridge Studies in Criminology, pp. 20-32). Cambridge: Cambridge University Press, https://doi.org/10.1017/CBO9780511499470.002.
- Matisen, T. (2019) *Kadenca – profesionalna autobiografija* (prevod dela: *CADENZA – A professional autobiography*, London, 2017, prevodilac: Vujanić-Đorđević, M.), Edicija CRIMEN. Beograd: Pravni fakultet Univerziteta u Beogradu.
- Milutinović, M. (1977). Penologija – nauka o izvršenju krivičnih sankcija i resocijalizaciji osuđenika. Beograd: Savremena administracija;
- Monaghan, J. (2012) Terror carceralism: Surveillance, security governance and de/civilization. *Punishment & Society, 15*(1), pp. 3-22, https://doi.org/10.1177/1462474512466197
- Mrvić-Petrović, N. (2022) Kako učiniti human(ij)im doživotni zatvor koncepta „zaključaj i baci ključ” na primerima Italije i Holandije. *Strani pravni život*, 3, pp. 403-428, https://doi.org/10.56461/SPZ_22304KJ
- Pollock, J. M. (2006) *Prisons: Today and Tomorrow*, Second Edition. Sudbury: Jones and Bartlett Publishers.
- Savet za štampu, available at: https://www.soinfo.org/vesti/vest/27552/savet-za-stampu-informer-ponizio-zrtve-i-uznemirio-javnost/
- Soković, S. (2011) Savremene globalne tendencije u kontroli kriminaliteta (karakteristike, perspektive i osvrt na domaće prilike. *CRIMEN, 2*(2), pp. 212-226;
- Solomon, E. (2008) Life-sentence Prisoners. In: Y. Jewkes & J. Bennet (eds.), *Dictionary of Prisons and Punishment.* Devon, Willan Publishing, pp. 153-155.
- Stojanović, Z. (2020) *Komentar Krivičnog zakonika,* Deseto dopunjeno izdanje. Beograd: Službeni glasnik.
- Turanjanin, V. (2021) Life Imprisonment Without Parole: The Compatibility of Serbia’s Approach with the European Convention on Human Rights. *Liverpool Law Review*, 42(4), pp. 1-32, doi:10.1007/s10991-020-09269-6

– World Economic Forum (2019), Prisons are failing. It’s time to find an alternative, available at: https://www.weforum.org/agenda/2019/01/prisons-are-failing-time-for-alternative-sparkinside/ page accessed on 01.03.2023.

Law sources

– Criminal Code, Official Gazette of the RS, No. 85/05, 88/05 – corr., 107/05 – corr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 and 35/19.
– Law on Execution of Penal Sentence, Security Measures and Educational-Corrective Measures, Official Gazette FNRJ, no. 47/51.
– Law on Execution of Criminal Sanctions, Official Gazette FNRJ, no. 24/61.
– Law on Execution of Criminal Sanctions, Official Gazette SRS, no. 26/77, 50/84, 46/86 and 16/87.
– Law on Execution of Criminal Sanctions, Official Gazette RS, nos. 16/97 and 34/01.
– Law on Execution of Criminal Sanctions, Official Gazette RS, nos. 85/2005 and 72/2009.
– Law on Execution of Criminal Sanctions, Official Gazette RS, nos. 55/14 and 35/19.
– Law on Penal Execution, Official Gazette FNRJ, no. 92/48.
– Recommendation Rec(2003)23 of the Committee of Ministers to member states on the management by prison administrations of life sentence and other long-term prisoners (Adopted by the Committee of Ministers on 9 October 2003 at the 855th meeting of the Ministers’ Deputies).
– Recommendation Rec(2006)2 of the Committee of Ministers to member states on the European Prison Rules (Adopted by the Committee of Ministers on 11 January 2006 at the 952nd meeting of the Ministers’Deputies)
– Standard Minimum Rules for the Treatment of Prisoners Standard Minimum Rules], RES/663 C (1957) and RES/2076 (1977) Adopted by the First United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held at Geneva in 1955, and approved by the Economic and Social Council by its resolution 663 C (XXIV) of 31 July 1957 and 2076 (LXII) of 13 May 1977, available at: https://www.unodc.org/documents/justice-and-prison-reform/Nelson_Mandela_Rules-E-ebook.pdf, page accessed on 15.02.2023.
– Temporary Instruction on Penal Execution (Cab. no.1199 from 27.september 1945).

Judical practice

- Corte Constitucional, Communicado 33, Septiembre 2 de 2021, Sentencia C-294/21
- ECHR *Vinter and Others v. the United Kingdom*, Nos. 66069/09, 130/10 and 3896/10, 09.07.2013.
- ECHR *Bancsók and László Magyar (no. 2) v. Hungary*, nos. 52374/15 and 53364/15, 28.01.2022.

prof. dr Aleksandra ILIĆ,
Vanredni profesor,
Fakultet bezbednosti
Univerzitet u Beogradu

ANALIZA NEKIH PROBLEMA U OSTVARIVANJU RESOCIJALIZACIJE KAO SVRHE KAŽNJAVANJA

U radu autor se bavi savremenim problemima u postizanju cilja resocijalizacije kao dominantne svrhe izvršenja zatvorske kazne u većini zemalja danas. Resocijalizacija je jedan od osnovnih principa na kojem se zasniva tretman lica osuđenih na kaznu zatvora i sastoji se od brojnih pravila postavljenih u određenim međunarodnim dokumentima, ali koje čine i deo nacionalnog zakonodavstva. U radu je dat pregled istorijskog razvoja modela resocijalizacije kako u svetu tako i kod nas, kao i savremenih pristupa u razmatranju te problematike. Autor dalje analizira neke retributivne tendencije u savremenom zakonodavstvu. Jedan od problema je trend izricanja doživotne kazne, što je posebno problematično u slučaju odsustva mogućnosti uslovnog otpusta za pojedine osuđenike. Taj oblik kazne doživotnog zatvora je propisan Krivičnim zakonikom Republike Srbije, pa autor razmatra održivost te odredbe, posebno u kontekstu odluka Evropskog suda za ljudska prava.

Ključne reči: resocijalizacija, zatvori, kažnjavanje, retribucija, doživotni zatvor

Muhittin DEMİRKASIMOĞLU, PhD*
CBRN specialist at the
Ministry of Health of Türkiye

Original Scientific Article
Received: 25 January 2023
Accepted: 8 March 2023
UDK: 351.773(560)
https://doi.org/10.47152/rkkp.61.1.6

EVALUATION OF HEALTH INTELLIGENCE STUDIES IN TURKEY SUMMARY

The last major epidemic, the COVID-19 pandemic, has revealed that there are many deficiencies in the health field. During the COVID-19 pandemic, as far as the media followed, many countries had difficulties accessing medical supplies, vaccines, and drugs and did not allow some medical products to leave the country. It has been observed that the necessary materials have disappeared with the work of the intelligence agencies of some countries. Politicians and scientists from many countries have put forth conspiracy theories about the source of the pandemic and the country of origin, and accusations have included claims about the use of biological weapons. This study aims to reveal what health intelligence is and what kinds of studies are done in Turkey and around the world. For this, the in-depth literature study of the case pattern study, one of the qualitative research methods, was used. In the analysis of the study, a descriptive analysis was made and the results were discussed.

Keywords: Intelligence, medical intelligence, cyber attack, biological weapon

* e-mail: mdemirkasimoglu@yahoo.com

1. Introduction

From the past to the present, intelligence/espionage constantly renews and develops itself in parallel with the technological developments of those periods. It determines the direction of many situations such as diplomacy, propaganda, psychological warfare, asymmetric threats, military power, economy, covert operations, and technological developments. In this context, intelligence helps to predict the intentions of rival countries/persons/institutions/unions/organizations, their existing power to realize these intentions, and possible measures they can take against counter-attack plans (Tiryaki, Özdal, 2020: 267). Strategic intelligence, which plays an important role in determining the policies and strategies of states in line with national interests, includes all elements of national power (Acar, Urhal: 2007: 209).

2. Situation in Turkey and the world

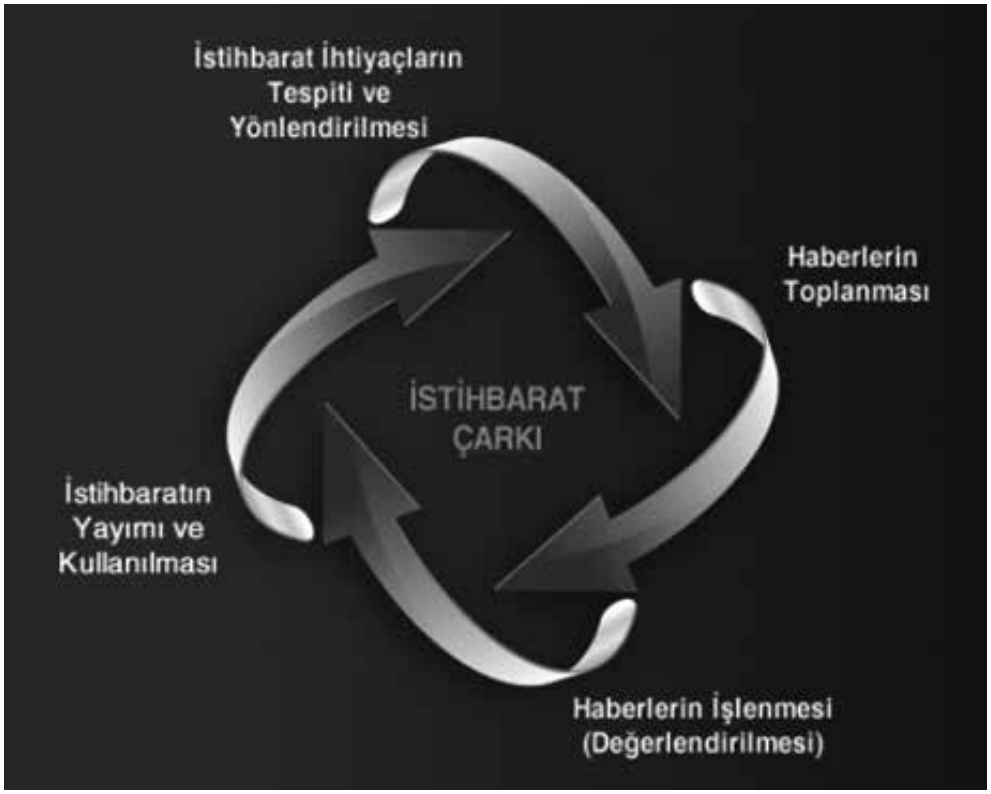
The introduction of the Internet into human life and the subsequent emergence of social media tools made it easier to gather open-source information in areas where intelligence and counterintelligence studies will be conducted. While users share much data, such as news, videos, pictures, and plain text, not only ordinary people do so due to the free nature of social media and its rapid spread capacity. In other words, it also offers an environment where propaganda can be made in social media environments, where terrorist organizations can easily gather sympathizers, and where open source intelligence (OSINT) can be provided to intelligence services. Open source-based data mining, artificial intelligence, and advanced algorithms that can solve complex networks (deep machine learning) are applied to big data, making it possible to reach many intelligence information (Özdağ, 2011: 24).

With the developments in information technologies, countries that try to collect the data obtained from many fields and turn them into intelligence, have tried to use them in favor of their countries against the country they perceive as a threat, not only in the military, economic, and political but also in all areas of life. The use of data and information obtained in the field of health as intelligence has become one of the most important hybrid threat areas in recent years.

It is only possible to see the future, have information about possible problems in advance, and reach the facts behind the scenes, only with a healthy intelligence production. In order to produce intelligence, it is not sufficient to collect news, information, and documents alone. The obtained news, information, and

documents should be processed in a certain, systematic way. If important news is not evaluated correctly, misleading results can be reached (MIT, 2021). The intelligence cycle; It is likened to a continuous wheel in the order of determining intelligence needs and directing collection efforts, collecting news, processing news, publishing, and using intelligence (Figure 1) (MIT, 2021).

Figure 1. The Intelligence Cycle



Source: https://www.mit.gov.tr 2021

Intelligence activities are multidisciplinary and multisectoral in health intelligence, as in many successful studies. All over the world, health threats are added to hybrid threats. The collected data and information are brought together and used in health technologies to spy on the health industry, and by using them in medical engineering, the required products are produced with reverse engineering applications. Similar studies confirm the above-mentioned statements about the products used by ISIS/DAESH militants during the occupation and defense of some cities in Iraq and Syria, with the joint efforts and means of their engi-

neers, health personnel, and other terrorists (Gambetta, Hertog, 2016:135). Again, as an example of terrorists' intelligence gathering, it is known that the Japanese Aum Shrinkyo sect obtained anthrax to use in the attacks, went to Africa to obtain the ebola virus, and voluntarily participated in the studies there to try to obtain the ebola virus. One of the best answers to the question "why is health intelligence important" is that millions of people have died due to epidemics throughout history, and these deaths can be prevented with healthcare products in the modern world. In the COVİD-19 pandemic (as of April 22), 6.2 million people died from the disease. Of the 10 major epidemics that caused serious deaths in history, the biggest loss was 75-200 million, with the plague epidemic called the black death (Tharoor, 2021:1). Some of the epidemics in history spread as terrorist activities, and some of them spread unintentionally as a result of commercial activities. Health intelligence studies are carried out to prevent these epidemics from entering the country quickly by being informed in advance, and to take effective measures if they cannot be prevented. The epidemics, with their size, lethality, and contagiousness, have caused the prices of goods and services in the health system to increase in terms of national and reserve currencies.

For the term health intelligence to be established, strategic intelligence must be understood. Although tactical and/or operational intelligence is used more effectively and frequently in the field, it cannot solve all kinds of problems, and tactical/operational intelligence solutions to strategic problems are insufficient. Since the facts are often multi-parameter, multi-faceted, and complex, it is not possible to understand and solve national or international problems with tactical intelligence information and plans. Elements such as biographical, telecommunicational, geographical, political, scientific, and technical intelligence, which are necessary for the formation of policies and military plans at national and international levels, are among the elements within this definition. To develop good strategies, strategic intelligence must also be done well and properly. Liebowitz (2006) defines strategic intelligence as intelligence that feeds and assists the strategic decisions of organizations, consisting of artificial intelligence, information management, business intelligence, and competitive intelligence (Smith, 1996:1).

The key points of medical intelligence are that it is an intelligence function, albeit one focused on medical matters and not a medical function, and that it applies to strategic and operational consumers. Today, countries' medical intelligence has been put to use in providing national security at the strategic, operational, and tactical levels (Kaufman, 2001: iii).

Strategic Intelligence: It is a type of intelligence that is used to investigate, detect, and predict future opportunities and threats for a state, to put options be-

fore decision-makers, and to ensure that their policy-making process is built on a more accurate basis. The purpose of strategic intelligence; is to reveal and determine the possibilities and capabilities, sensitive and weak sides, and possible reactions of the target country or countries in advance (Yılmaz, 2007:34). Özdağ's (2002:112) medical intelligence assessment; he evaluated medical intelligence as a type of intelligence that can be used mostly by military planners, with the definition that "information collected from foreign medicine, biology, and environmental science sources about rival armies and the battlefield and which will be useful to military planners falls within the scope of medical intelligence". Medical intelligence includes the following subjects in terms of the operations to be carried out by the armed forces of the states (Bolin, 1989: 12/50):

- Common and communicable diseases, quality and availability of health services,
- Number of medical supplies, medical services, health service facilities, and trained health personnel,
- Regional special diseases, bacteria, insects, snakes, fungi, harmful vegetation, and other harmful organisms,
- Foreign animal and plant diseases, and especially diseases transmitted from them to humans,
- Health problems related to the use of local food sources,
- Medical effects and protection against chemical, biological agents and radiation,
- Newly developed foreign weapon systems and their effects on health,
- Special medicines and vaccines used by enemy forces,
- It includes geographic information such as altitude, heat, cold, sandstorms, and swamps of the operation area that may affect the health of personnel.

Some of the medical intelligence includes a country's cell culture collection, a list of selected agents, a phage database, and its contents. It also includes information about the microbiological agents that affect human health and are specific to the region, what are diagnostic tests, prevention methods, vaccines, antiserum, and treatment methods.

It is to produce intelligence information that includes foreign countries' military and civilian medical capabilities, treatment institutions, medical personnel, emergency and disaster response capabilities, logistics, and medical industry stages. To create an integrated database of all therapeutic, educational, pharmaceutical, and research facilities (NATO, 1999:32-33).

Medical intelligence epidemiologically, in terms of military forces, is to collect, compile, and present information about all infectious diseases that may threaten the health of the troops to be sent to the duty area. It is to rate the effects of long-term health problems and infectious disease risks on the soldiers performing duty and to prepare reports about these ratings and evaluations. To profile endemic diseases and recommend measures to be taken for the support and protection of military units (Tümer, 2022: April 13th).

Medical intelligence helps assess the impact of trends and currents that may affect environmental health, environmental safety, and national policies. In the medical intelligence unit; There should be specialist personnel from departments such as public health, epidemiology, military health services, infectious diseases and clinical microbiology, microbiology, nuclear medicine, medical CBRN, medical biochemistry, environmental health, toxicology, psychiatry, and biomedical engineering. Entomology and zoology, health sciences such as veterinarians and pharmacists, sciences such as genetics, environment, forestry, agriculture, geology, meteorology, electronics, computer engineering, and Weapons of Mass Destruction (WMD) should be strengthened by working in coordination with the armed forces and civil defense institutions. Medical intelligence, like other types of intelligence, uses the process known as the “Intelligence Wheel”, which shows the stages of transforming raw information into intelligence. This process ncludes determining and planning the intelligence needs, collecting the necessary information and news, classifying and analyzing the collected information and news, briefly processing, distributing the intelligence to the necessary institutions and people, and using it. Identifying and Directing Intelligence Needs: This is the first stage in which the medical intelligence agencies determine the news-gathering environments and direct the news-gathering activities in line with these requests and needs, against the intellectual demands of the state decision-makers on medical issues. News Gathering: The news gathering function, which is one of the most important stages in the medical intelligence formation process, is carried out by using “open” and “closed” sources. Books, radio, television, newspapers, scientific articles, and internet sites can be shown as open sources. Closed sources, on the other hand, consist of people who can gather news on a specific intelligence need, using technology as well as various news-gathering methods. The collected medical intelligence should be delivered to the requesting unit as soon as possible.

Processing (Evaluation) of News: At this stage, the collected medical information is classified, evaluated, interpreted, and analyzed. Dissemination and Use of Intelligence: Reports that have been analyzed and turned into intelligence

are delivered to the relevant persons and institutions in a timely and rapid manner. In addition to using this intelligence, relevant persons and institutions determine their new intelligence needs within the framework of new variables and priorities. As seen in the SARS in 2003 and the flu epidemics in 2009, infectious diseases cross international borders without difficulty (Bolin, 1989: 6-38/50). The Crimean-Congo Hemorrhagic Fever is the same in Turkey.

Strategically medical intelligence contributes to the formation of national and international policies of states based on the medical or biological scientific capabilities of foreign military and civil societies (Bolin, 1989: 20/50).

Medical intelligence conducts studies on medical, hygienic, and environmental conditions in some strategically important areas. These studies include an assessment of significant potential diseases, industrial accidents, and local medical personnel, medical facilities, training programs, and research institutes. Mobilizing military doctors in a country, purchasing more medical supplies than ever before, storing too many vaccines, serums, and antibiotics, increasing the capacity of blood banks and relocating them, drug stocks, and any intelligence in health policies are important in determining the intention of the target country. The fact that any state begins to vaccinate its citizens or soldiers against a special infectious agent is a sign that it has the biological capability or is trying to develop its biological warfare capability by planning an attack against another state (NATO, 1999: 32-33).

Their targets are human hearts! The devil's unthinkable infiltration attempt, however, the vulnerability displayed in an insulin pump last year (the year 2021) revealed that attacks can threaten the lives of patients. When it was revealed that attackers could give double doses of drugs to patients due to security vulnerabilities, the frightening extent of these neglects in the field of security caused controversy. It is a matter of curiosity whether pacemakers or medical devices produced with newer technologies are at risk. Experts argue that security measures should be increased regarding these devices where human life is at stake. A study conducted last year revealed that more than 80 percent of health institutions have encountered security incidents in information technologies, that is, devices connected to the Internet, in the last 18 months (Kocabaş, 2022: June 6th). Widespread healthcare monitoring provides rich contextual information to address the peculiarities of chronically ill patients. Continuous monitoring and early medical intervention not only improve the quality of life of the elderly and people with chronic diseases but also assist families and parents by providing high-quality healthcare to their young infants and paralyzed children. While the importance of

Wireless Body Area Networks (WBANs) is indisputable, the amount of data produced by these sensors is huge and includes computing, memory, communication power, massive storage infrastructure, energy-efficient performance for processing, real-time monitoring, and data analysis. This is a system that has not been fully secured and has some security vulnerabilities (Masood et al., 2018: 23).

Legislation; When the legislation is scanned, the law enacted for intelligence in Turkey is seen as the only one, and it was enacted as the National Intelligence (MIT) Law. According to the State Intelligence Services and National Intelligence Organization Law (Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu, Resmî Gazete, 1983); Article 4. subparagraph i; To search for information, documents, news, and data by using all kinds of technical intelligence and human intelligence procedures, tools, and systems on foreign intelligence, national defense, counter-terrorism, international crimes, and cyber security, to collect what is researched, to record, analyze, and evaluate what is collected and to transmit the generated intelligence to the necessary organizations. Article 4. Subparagraph J is to be ensured that the appropriate data and information are provided by following the technological developments, by researching modern intelligence procedures and methods to increase the quality and capacity, quality and effectiveness of the Intelligence. All ministries are given the task of collecting intelligence, reporting to MIT, and countering Intelligence. It imposes obligations on ministries in these matters. In addition, only four regulations on intelligence have been issued. The purpose of the “Regulation on the Public Disclosure of the Reports Prepared as a result of the Inspection of State Property of Public Administrations Regarding Defense, Security and Intelligence” published in the Official Gazette No: 28385 is aimed at the Ministry of National Defense, the Undersecretariat of the National Intelligence Organization, the Undersecretariat of Defense Industries, the Undersecretariat of Public Order and Security, the General Secretariat of the National Security Council, the Gendarmerie General Command, the Coast Guard Command and the General Directorate of Security (Savunma, Güvenlik ve İstihbaratla İlgili Kamu İdarelerinin Devlet Mallarının Denetimi Sonucu Düzenlenen Raporların Kamuya Açıklanmasına Dair Yönetmelik, Resmi Gazete, 2012).

The purpose of the “Turkish Armed Forces, National Intelligence Organization, General Directorate of Security, Gendarmerie General Command, and Coast Guard Command Movable Property Regulation,” published in the Official Gazette No. 27652, regardless of the source and acquisition method, is the registration of movable properties in the hands of the relevant institutions, their removal from the records, their management and internal audit procedures and princi-

ples, and the determination of duties, powers, and responsibilities (Turkish Armed Forces, National Intelligence Organization, General Directorate of Security, Gendarmerie General Command and Coast Guard Command Movable Property Regulation, 2003). The aim of the "Revenue General Directorate of the Ministry of Finance, Tax Intelligence Specialist Duty, Authority, Work and Appointment Regulation," published in the Official Gazette No. 22873, is to ensure that the members of the profession are recruited, trained, and promoted in the profession, their duties and powers; The relations with the General Directorate of Revenues, regional directorates of revenues, tax intelligence directorates, and other relevant units, as well as working procedures and principles are regulated (Maliye Bakanlığı Gelirler Genel Müdürlüğü Vergi İstihbarat Uzmanı Görev, Yetki, İş ve Atama Yönetmeliği, Resmi Gazete, 1997). The purpose of the "Regulation on the Meeting, Working Principles and Procedures of the Smuggling Intelligence Coordination Board," published in the Official Gazette No. 19624 is to evaluate and combat all kinds of smuggling activities in Turkey and abroad and to assist in the determination of target tactics and procedures. It regulates the meeting, working, principles, and procedures of the Smuggling Intelligence Coordination Board in the Central Establishment of the Ministry of Interior to ensure coordination between institutions and organizations and to carry out services. Apart from these, other legislation related to intelligence could not be reached from open sources (Kaçakçılık İstihbarat Koordinasyon Kurulunun Toplantı, Çalışma Esas ve Usulleri Hakkında Yönetmelik, Resmî Gazete, 1987).

Legislation on espionage in various fields has been enacted in the USA. It has legislation in a wide range of areas, from espionage in the economic field to espionage and intelligence in the field of health. The European Union (EU) issued a new regulation, Regulation (EU) 2022/123 of the European Parliament and the Council, in January 2022 for medical products and medical devices (The European Parliament And Of The Council, 2022). It was also requested that these products be protected from copyright and espionage. In the USA, legal regulations on intelligence and espionage have been developed with the presidential order issued after 2001 and additional articles to the public health law. Since the regulations in some areas are confidential both in Turkey and the USA, they can not be accessed from open sources.

3. Material method

For this study, the "in-depth literature review" study of the "Situation Pattern" study, which is one of the qualitative research methods, will be used. Ethics

committee approval was not obtained as there was no study to obtain ethical committee approval. Qualitative academic studies are one of the best research methods used to conduct scientific studies on subjects that are necessary for the field of health but cannot be quantified with numerical data. According to Davey, this study, out of 6 studies, they are descriptive, called Illustrative Case Studies, and uses one or two case studies to give information about a situation (Davey, 1991: 2). According to Bogdan and Biklen (Bogdan and Biklen, 1998: 135), 8 types of case study documents are the main data source; As part of a case study with participant observation or interview, the term document is used as supplementary information to refer to materials such as photographs, videos, films, notes, letters, diaries, clinical case records, and memories of all kinds. Documents are the primary data source of document review work. When discussing this form of work under the heading of qualitative research, the degree to which a particular study fits the description depends on the information presented in the first chapters, how the research is conducted, and how flexible the definition of qualitative research is. The documentation meets the criteria for using definition-rich data. However, to what extent the researcher uses them, this naturalistic, inductive, and descriptive case study from the case design is the only case, in health intelligence that has been examined. In the first stage of the study, the problem was identified and the aim was determined. In the second stage, the research method was determined, and the data collection method and in which databases to search were decided.

At this stage, exclusion and inclusion criteria were also determined. Scans were made in the databases determined in the third stage, and sources are listed according to inclusion/exclusion criteria. In the fourth stage, it was decided which of the sources obtained in the systematic review would be used. Resources are classified in terms of content. In the fifth and last stage, the data were subjected to in-depth content analysis, and the study was reported. In the study, purpose-oriented data were collected to facilitate the analysis in the data collection process, and basic research words were used in order not to get lost among the data during the analysis process. The gap analysis was evaluated by reviewing the data, criticisms, and deficiencies. In this respect, the data has been tried to be enriched as much as possible. “How many documents should be looked at?” Although it is a legitimate question, the concern should not be about ‘how many’; rather, given the purpose and design of the study, it should relate to the quality of the documents and the evidence they contain. Document analysis is more than simply arranging a series of extracts from printed material to convey whatever idea comes to the researcher’s mind. Rather, it is the process of evaluating documents in an environment where empirical knowledge is produced and understanding is developed (Bowen, 2009: 27-29).

The data were separated according to their types and collected according to this structure. In the data collection process, how the data was collected is explained. When the data analysis process was started, a literature review/resource review was made again for the data whose deficiencies were felt while performing the data analysis. In the data analysis process, the need for data was determined according to the design for the development of the data model, and the analysis was continued by collecting data accordingly. Searches were made from places such as Google Scholar, YÖK thesis, Pubmed, NCBI, ProQuest, web of science, Dergipark, Turkish legislation site, Yandex, and Hacettepe library. These were chosen as the research universe. Research limitations, health intelligence is not well known, it is confused with public health intelligence in this field, and there are very limited resources in Turkish. In English, the words “intelligence” and espionage are confused. While searching, the word “intelligence” in English also meant intelligence and intelligence, and as a result, causing some confusion, many studies were excluded from the study.

Legislative review was conducted for Turkey. In Turkish, the words istihbarat, stratejik istihbarat, açık kaynak istihbaratı, espiyonaj, istihbarata karşı koyma, sağlıkta siber saldırılar, sağlık istihbaratı, sağlık espiyonajı, stratejik istihbarat, sağlık istihbarat mevzuatı, istihbarat kanunu, istihbarat yönetmeliği, sağlık istihbaratı yönetmeliği were searched. Searches were made with the words Intelligence, espionage, countering intelligence, Medical Intelligence, Health, Intelligence, Intelligence legislation, Health Intelligence legislation, cyber attack, open source intelligence, strategic intelligence in English.

Table 1. *Included and Excluded Total Resources Scanned by Languages*

Language	**Included**	**Excluded**	**Total**
Turkish	16	69	137
English	24	178	281
Total	40	247	418

In the literature review, a total of 418 resources required for the study were found. According to the literature review in Table 1, 137 documents were found. In the English literature search, 281 documents were found. It has been obtained from Turkish sources such as articles, books, reports, websites, and theses. The breakdown of these documents is as follows. From English sources, the weight is in the articles, the website, thesis, books, and reports have been examined. In Table 2, 229 references were included in the study according to the criteria of exclusion and inclusion of Turkish and English sources.

Table 2. *Data included in the research from the data obtained through the literature review*

Language	Included in the Research	Excluded from Research	Total
Turkish	13	21	57
English	11	140	172
Total	24	161	229

The exclusion criteria excluded from the study were those that appeared in another search of the same publication, other than human health, those about public health information sources, only surveillance systems, and only early warning systems. Inclusion criteria; First of all, general intelligence information, information describing health intelligence, public health information related to intelligence, surveillance and early warning systems related to intelligence, strategic intelligence, and all information related to humanity.

Table 3. *Distribution of sources included in the studies*

	Books	Article	Report	Web sites	Thesis	Total
Language						
Turkish	13	21	4	6	13	57
English	11	140	12	6	3	172
Total	24	161	16	12	16	229

As a result of the in-depth examination of the sources obtained in the studies in Table 3 and the evaluation made with data analysis, the sources used in the distribution of resources are presented in Table 4. Data analysis was performed according to Table 4.

Table 4. *Distribution of resources included in the studies*

	Books	Article	Report	Web sites	Thesis	Total
Language						
Turkish	5	12	2	4	6	29
English	3	42	8	2	2	57
Total	8	54	10	6	8	86

4. Findings

The legislation issued for intelligence in Turkey has been scanned. As far as can be determined from open sources, it has been observed that only one law, and four regulations other than the law, have been issued. It is estimated that there is enough covert legislation with the State Intelligence units themselves, and enough secret legislation that cannot be known with clear legal regulations obtained from open sources. There is a directive regarding health, and it is stated that health-related intelligence should be made in the duties and responsibilities section of this directive. This situation is similar around the world. Only in the USA, especially after the September 11, 2001 attacks, are legal data available from open sources on the need to conduct intelligence studies in the field of health and contribute to the security of the country, with the Public Health Law, the Patriot Act, and the Presidential Order. All data obtained in this study were obtained from open sources. Health intelligence studies in Turkey and some other countries in the world have been extensively researched, and the data obtained has been examined in depth. The analyzed data were filed one by one. Descriptive analysis was carried out under certain systematics.

There are different perspectives on the definition of validity in qualitative research and the terms used in making this definition. Among these perspectives, in qualitative research, examining validity in terms of its quantitative equivalents, using terms suitable for the qualitative paradigm unlike the quantitative approach, downplaying validity, combining or synthesizing different perspectives, or visualizing it metaphorically can be counted (Creswell, 2007: 128). In this study, construct validity was created in the literature review, and the chain of evidence was created during the data collection phase. Internal validity was done during data analysis with construct definition. External validity was obtained by the design of the research in a single case study. Thanks to the development of databases, reliability has been ensured in the data collection phase.

5. Discussion

According to Özdağ, armies covered longer distances faster with the use of telegraphs, telephones, railways, armored vehicles, and weapons with great destructive power as of the 19th century. As a result of the rapid development of science, technology, social structure, and the understanding of threats in different dimensions, every moment of life has been the subject of intelligence. To resist such developments, intelligence began to be collected not only during the war but also before the war (Özdağ, 2011: 55).

Is health intelligence just the process of getting the news of biological attacks in advance? Does it mean the seizure of existing personal data? Personal data is meant only for data on how large a population is or for data on very important persons. Health intelligence is a key hurdle and main driver for initiatives like precision medicine. Personalized healthcare is a disease management approach that takes into account individual variability in the environment, lifestyle, and genes of each person. The National Institutes of Health (NIH) aims to pioneer a new model of patient-supported research to develop healthcare solutions, people who make the best decisions to prevent or treat a disease, predict outbreaks, and improve quality of life. Clinicians and public health practitioners can use technology to deliver the best evidence-based tailored treatments or interventions to sustain high-quality patient care and build healthier communities (Shaban et al., 2018: 53). When using artificial intelligence, we can determine the health of society and critical personnel or get information about the management by going from general to specific. Preventive medicine tries to define the issues that constitute medical threats, evaluates the risks that will occur when exposed to these threats, and works on measures to prevent aggravation. Medical intelligence, it identifies medical threats, and also helps states determine their policies and interests, and directly ensures national security, by assessing medical trends, organizations, and related events that directly or indirectly affect foreign societies that may come to our attention and influence our policies (Kaufman, 2001: iii).

65% of the US soldiers who operated on Togatabu Island in 1942 contracted a disease called “filariasis” carried by mosquitoes and were weakened by the disease, not by enemy attacks (U.S. Army, 2000: 1-3). At this time of increasing concern about deadly and costly infectious disease threats posed by natural disasters or bioterrorism attacks, preparedness, early detection, and timely response to emerging infectious diseases and epidemics are an important public health priority and an emerging field of multidisciplinary research. Public health surveillance has been practiced for decades and remains an indispensable approach for detecting emerging disease outbreaks and pandemics. Early knowledge of a disease outbreak plays an important role in improving response effectiveness. Computer-based surveillance systems enable rapid public health response by real-time or near-real-time detection of serious diseases and potential bioterrorism agent exposures. The rationale behind syndromic surveillance lies in the fact that certain diseases of interest, such as nurse calls, medication intakes, and absenteeism from school or work, can be monitored with timely syndromic presentations. The important thing is to establish a strong system. In this case, if the usage deficiencies are reinforced with other systems and supported by surveillance, leaks will be

prevented. Thus, part of a strong public health intelligence system will be established. Data privacy, security, and access control are among the core research and development topics. An access control mechanism based on data privacy and user access privilege is implemented. While syndromic surveillance has been widely accepted as a response to disease outbreaks and bioterrorism attacks, many research challenges remain. The potential benefit of syndromic surveillance regarding timely detection is that timely detection cannot be achieved if hundreds or thousands of people are infected at the same time. In extreme cases, modern biological weapons can easily lead to mass infections through the air or water-borne agents. In particular, how to deal with incomplete data records, how to perform privacy-conscious data mining, and how to exploit multiple data streams are all interesting research questions. In addition, a comprehensive evaluation of epidemic detection algorithms using synthetic or real data is critically required. Outbreak detection algorithms need to be improved in terms of sensitivity, specificity, and timeliness. In addition, a comprehensive evaluation of epidemic detection algorithms using artificial or real data is critically necessary (Yan, Chen, Zeng, 2008: 33-37).

Mossad attempts to analyze Hafez Assad's urine, to determine which drugs he took, to make inferences from the drugs he used, to try to predict how much life he has left and what he will do about the Golan Heights in the rest of his life (Özdağ, 2011: 123; Hurriyet, 2000: January 10th). It is known that the treatment of Iranian Shah Mohammad Reza Pahlavi, who had cancer since 1973, by French doctors, hiding his illness and not being able to learn that he had cancer by the USA, caused one of the most important foreign policy crises of the USA (Mcdermott, 2007: 501).

Leaving antibiotic-resistant bacteria in intensive care units is a hybrid attack. It can cause the death of critically ill patients with microorganisms with high antibiotic/antiviral resistance. Physicians will find it difficult to save patients, and as a result, social fear will increase. Some of the most important sources to refer to in open-source intelligence in health are scientific publications. Intelligence services in many countries have always used the information obtained by working with academics, making them intelligence officers, questioning business travelers and tourists, and examining domestic and foreign press and publications. Publicly available books, periodicals, advertisements, catalogs, and brochures are analyzed for open-source intelligence. In addition to these, radio, television broadcasts, and the internet are also shown as data sources (Friedman, 2002: 18).

Beyond disseminating the ideas and discourse of emergency preparedness, this reflects an emergent effort to cultivate electronic communication about health

events. As such, it illustrates a key and novel dimension of contemporary public health intelligence (PHI). A central aim of contemporary PHI is the detection of health events as (or even before) they unfold. In the early 20th century, 'epidemiological intelligence' was gathered by health organizations – e.g. regional bodies operating under the auspices of the League of Nations – through a variety of media, including 'wireless broadcast; telegraph; and weekly tabled publications' (Bashford 2006: 73). Today, digitized media have inspired technoscientific imaginaries that render these older media arcane; whereas the intelligence systems of the early 20th century aimed at being 'current' (Lothian, 1924), those of the early 21st century are directed ahead of the current. Aspiring towards this pre-emptive ideal means extending PHI beyond traditional activities, such as epidemiological surveillance and the systematic tabulation of case reports, into non-traditional activities such as blogging and data-mining in electronically mediated social networks. To the extent they get people communicating about the health events they perceive, these non-traditional activities constitute a potential treasure trove of health-relevant information. Accordingly, Kahn (2011) is engaged not just in cultivating public communication about the zombie apocalypse and other health events, but also in exhorting public health organizations to prepare to mine this treasure trove for PHI. Capitalizing on the 'wisdom of crowds'– leveraging the public's communication about its embodied interactions with health-altering exposures – is thought to require significant transformations in public health (cited in French, Myhalovskiy, 2013: 175).

The decentring of traditional epidemiological concerns is matched by a parallel shift in the forms of knowledge now being privileged in PHI. At the global level, this shift can be conceptualized in terms of the relationship between official and unofficial sources of knowledge. Whilst sociologists have long been concerned to understand the contested place of knowledge – especially lay knowledge – in the production of medical truths, little attention has been paid to the incorporation of unofficial forms of knowledge into PHI apparatuses. Could the use of disinformation, misinformation, and multiple data in health intelligence and counter-intelligence processes be perceived as an attack on the public's free choice or information, to combat them? The first area in the fight against disinformation is primarily concerned with where and how data will be collected. Related topics include data entry approaches, data sharing protocols, and transmission techniques (Weir, Mykhalovskiy, 2010: 153).

One consequence of this incorporation and formalization of unofficial knowledge has been the ballooning of initiatives experimenting with different kinds of 'infodemiological' techniques and technologies (Eysenbach, 2009: 6).

The second area introduces modeling, analysis, and data mining approaches to track data anomalies and discover whether the abnormal data state is due to a real change in disease occurrence. A critical step between data collection and abnormality detection, the syndrome classification process focuses on classifying raw, observational data into syndrome groups to provide evidence for detecting deviations in any monitored disease. The third area includes data visualization, user interface, and information dissemination functions. Public health officials, epidemiologists, emergency response and homeland security personnel, if necessary, gather information needed to access detailed information for further investigation, gain situational awareness, alert generation, response planning, and incident management; interacts with syndromic surveillance systems through these components to make decisions about dissemination.

Are there issues to be considered in health intelligence now that digitalized medical devices are under attack? Should drug, vaccine, antisera production, employees, and laboratory processes be added to intelligence data collection activities and counter-intelligence processes? The World Health Organization (WHO) may not be the first organization that comes to mind when the topic of cyber espionage comes up, but criminals and even nation-states have some compelling reasons to target it. Non-public insider information about therapeutic drugs or vaccines in development, and unfiltered information about the progress of the pandemic in various countries where WHO staff may be private can be valuable. Phishers and scammers often pretend to be WHO to solicit donations or try to redirect targets to malware sites; so much so that the organization has issued a public warning about attempts to compromise (Ikeda, 2020). The first English-language report on an atypical outbreak in China was published by a pharmaceutical company in the finance section of a newspaper reporting increased sales of antiviral drugs (Dion, AbdelMalik, Mawudeku, 2015: 210).

To carry out intelligence studies on national security in the field of health, it is necessary to be aware of it and work on it. No study has been conducted on health intelligence from the health community in Turkey. Awareness has not arisen apart from some newspaper reports and a few studies by some people outside the health sector (Tümer, 2022: April 13th; Ünlü, 2020: May 23rd; Seren, 2021: May 13th; Özcan, 2020: Apr 14th; Babacan, 2021: Jan 10th). In the field of public health, although some publications have been made only within the scope of medical precautions and protection measures regarding the source of the epidemic, scientific and academic studies have not been conducted in the field of Health Intelligence, which is the subject of this study.

According to the BBC investigation, Russia launched a massive media campaign in Georgia to slander the US-funded Public Health Research Center Richard Lugar (Lugar Center, Public Health laboratories research center, Tbilisi, Georgia) (Lentzos, 2018: Nov 19th). As a result of a public opinion poll, the authors and colleagues concluded in a recent study paper that a large proportion of respondents in Georgia believed that the Lugar Center was used or unstable for US-led research on biological weapons (Buckley, Clem, Herron, 2020: Apr 16th). Even though the Lugar Center is the country's primary testing facility for COVID-19 and is notable for being presented as the source of the virus by the Russian government's disinformation effort presented by Georgian media, the COVID-19 pandemic is an information epidemic when large amounts of accurate and misleading information spread rapidly over the internet (Cockerel, 2020: Mar 18th; Glasdam, Stjernswärd, 2020: 4).

COVID-19 has exposed serious problems and gaps in government defense systems, government capabilities, and information policy. More importantly, it revealed that the perception of national security should be revised. It has been revealed that a pandemic that is difficult to combat with conventional weapons can pose a greater threat to humanity. Analyses have shown that the development of an effective national response to COVID-19 must begin with the implementation of a coordinated pandemic information management plan. The phenomenon of disinformation plays an important role in managing the pandemic crisis.

Global exercises simulating the emergence of a pathogen with pandemic potential, to address the challenges faced by many countries in coordinating a multisectoral response to public health threats, between human, veterinary, agricultural, local, national, and international authorities. It will be necessary to update policies and ways for efficient information exchange. This approach will lead to higher resilience in countries during a pandemic and better logistical readiness for the distribution of food, drugs, protective equipment, diagnostic kits, vaccines, and therapeutics while preserving social structure and peace (Valdivia, Richt, 2020: 481). The challenges of using Electronic Data (ED) data for biosurveillance include relying on free text data (often the main complaint). Issues with textual data are handled in a variety of ways, including pre-processing the data to clean up text entries and handle negation. Using ED data for public health surveillance can significantly increase the speed of detecting, monitoring, and researching public health events (Waller et al., 2011: 53). The news that the measles disease started to spread among the Syrian refugees who fled the events in Syria and took shelter in Turkey was reported in the media (Milliyet, 2013: Sept.24th).

6. Conclusion

As a result, this study revealed that health intelligence studies in Turkey are insufficient, and the academic world of the country needs to do more work. Especially, Big-Data studies on health espionage/intelligence will make a serious contribution both in scientific terms and in the protection of the health of the people of the country. Health intelligence is not only the duty of intelligence agencies but also falls within the duty of all health professionals, health academics, and health bureaucrats. In the field of health intelligence, studies should be carried out primarily by university public health departments and the Ministry of Health. It will be developed systematically with academic studies to be done, and it will help with the issues of what is allowed in the field of health intelligence and what is not, and who should be more careful.

All over the world, academics, journalists, bureaucrats, and health facility managers collect health intelligence information. These intelligence studies are carried out not only for spying but also for system development. Regardless of the purpose, health intelligence studies should be carried out systematically, studied, and methods should be developed. This field will also open a new academic field for the academic community in the world, especially in Turkey. Criminal investigations of bioterrorism attacks, tracking of disease outbreaks, and medical intelligence operations require mission-oriented and mission-specific bioinformatics applications. A strategy must be formulated that embraces the needs of the forensic and medical intelligence communities to use genomic information in data exchange, and analysis systems. The National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI) require ensuring the secure transmission of classified and unclassified data while coordinating, managing, and improving existing biological defense operations within the National Biological Surveillance (US Army, 2008: 6).

The COVİD-19 pandemic has seriously disabled the existing conspiracy theories in this field and has shown that evidence-based studies are emphasized. Masks stolen at the Kenya airport, test kits that are not allowed to be sold, test kits with low reliability, insufficient intensive care respirators, and controlled sales of PCR devices to certain countries have revealed the importance of intelligence in many areas. Public health requires greater transparency in intelligence systems. A culture of innovation and change is demanded, as is a highly coherent policy and process development, evaluation, implementation, and dissemination strategy in Turkey’s public health system. Public health intelligence cannot be treated the same way as national/military intelligence – it must be treated on a highly

protected, highly secure, and need-to-know basis. What will be hidden, and what will not be hidden? The presence of the disease should be explained, and how it was detected can be explained. But for those who do, what kind of capacity and abilities can be hidden? Because the disease should not hit us. Or other countries should be prevented from hiding the disease. To do this, public health experts must make academic publications on health intelligence and public health intelligence. The study revealed that there are serious deficiencies in this area.

Health Intelligence, cyber security, medical intelligence, counterintelligence, strategic intelligence, open source intelligence, CBRN threats, early warning systems, and surveillance systems have been examined with descriptive data analysis. Although health intelligence is the broader definition, the term medical intelligence is used more. Public Health Intelligence primarily aims to obtain the information required for the protection of public health and to help ensure that protection and control measures are taken quickly for society. Early warning and response systems need to be strengthened and integrated with other institutions. To take countermeasures against intelligence in health intelligence, there is a need to increase awareness about the phenomenon of health intelligence. There is a need to strictly implement the principle of “must-know, need-to-know” in intelligence, and intensify studies on health intelligence and countering intelligence in health among health professionals, especially public health experts. There are health intelligence studies conducted by researchers outside the health sector in Turkey.

On the subject of Health Intelligence, those working in the public health sector and those working at the academic level should work with more publications and inform the health sector and the public. “Being aware” is the most important success process in health intelligence and intelligence opposition processes. These processes can be improved with further studies. The health intelligence work of a few people is an expression of the inadequacy in this area, similar to the way blind people describe it by touching an elephant. These studies have revealed that there is a need for serious studies in the field of health, especially in public health, and that coordination and coordination are essential in the intelligence institutions and health sector. Final note: Although this publication was sent to the journals publishing in the field of public health in Turkey, “no medical journal” was interested in the content of this article. This situation revealed that serious awareness studies should be carried out for the academic world in Turkey.

Literature

- Acar, Ü., Urhal, Ö. (2007) İstihbarat, *Devlet, Güvenlik, İstihbarat-Terörizm*, Ankara, Adalet Yayınevi, str.191-309.
- Babacan, N. (2021, January 10th) Hürriyet Gazetesi, Erişim available at: https://www.hurriyet.com.tr/ yazarlar/nuray-babacan/covid-19-biyolojik-bir-silah-mi-tibbi-istihbarat-birimi-olusturulmali-41593038, access on, 21.11.2022
- Bashford, A. (2006) Global biopolitics and the history of world health. *History of the Human Sciences*, 19, 1, pp.67– 88. https://doi.org/10.1177/0952695106062148
- Bogdan, R.C. & Biklen, S.K. (1998) Eleven Common Questions about Qualitative Research, *Qualitative research for education: An introduction to theory and methods* (3rd Edition). Boston, Allyn and Bacon. pp.39.
- Bolin, R. (1989) Medical Intelligence, *FM 8-10-8 Medical Intelligence in a Theater of Operations*, U.S. Department of Defense, Washington DC., available at: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1087&context=dodmilintel, p.1-50, access on 02.11.2022.
- Bowen, G. (2009) Document Analysis as a Qualitative Research Method*, Qualitative Research, Journal*, 9(2):27-40, https://doi.org/10.3316/QRJ0902027 available at: https://www.researchgate.net/publication/240807798_ Document_Analysis_as_a_Qualitative_Research_ Method, access on 14.11.2021.
- Buckley, C., Clem, R., & Herron, E. (2020) National security implications of the COVID-19 crisis: The urgent need to build state capacity, *Minerva Research Initiative*, available at: https://minerva.defense.gov/Owl-In-the-Olive-Tree/Owl_View/Article/2152823/ national-security-implications-of-the-covid-19-crisis-the-urgent-need-to-build/ , access on 20.01.2022.
- Cockerel, I. (2020) War on Science, March 18. (2020), available at: https://www.codastory.com/waronscience/lab-georgia-coronavirus/, accessed on 11.02.2022.
- Creswell, J.W., (2007) Five Qualitative Approaches to Inquiry, *Qualitative inquiry and research design: Choosing among five approaches*, *(2nd ed.). Sage Publications, Inc.* Thousand Oaks, California*, pp. 53-84.*
- Davey, L. (1991) The Application of Case Study Evaluations, Practical Assessment, Research, and Evaluation: Vol. 2 , Article 9. DOI: https://doi.org/10.7275/02g8-bb93, Available at: https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1031&context=pare, access on, 14.12.2020.

- Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu, 03.11.1983, Resmî Gazete, 18210, available at: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2937&MevzuatTur=1&Mevzuat Tertip=5, access on, 04.10.2022.
- Dion, M., AbdelMalik, P., & Mawudeku, A. (2015) *Big Data and the Global Public Health Intelligence Network* (GPHIN), *Canada Communicable Disease Report (CCDR)*, September 3, 2015, Volume 41-9, pp.209-214, available at: https://doi.org/10.14745/ccdr.v41i09a02, access on 12.10.2022.
- European Parliament and Union (2020) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022, retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32022R0123, accessed on: 14.12.2022.
- Eysenbach, G. (2009) Infodemiology and infoveillance: framework for an emerging set of public health informatics methods to analyze search, communication and publication behaviour on the internet. *Journal of Medical Internet Research*, 11, 1, pp.1-10, 10.2196/jmir.1157 available at: http://www.jmir.org/2009/1/e11/, access on 18.10.2022.
- French, M. & Myhalovskiy, E, (2013) Public health intelligence and the detection of potential pandemics*, Sociology of Health & Illness*, *35*(2), ISSN 0141–9889, pp. 174–187, https://doi.org/10.1111/j.1467-9566.2012.01536.x, Access on, 26.10.2022.
- Friedman, RS. (2002) Review Essay - Open Source Intelligence, *NATO Open Source Intelligence Reader*, available at: https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL %20Oct2002.pdf, access on 26.02.2022.
- Gambetta, D., Hertog, S., (2016) Mind- sets for Extremists. In: *Engineers of Jihad*. Princeton, New Jersey: Princeton University Press, pp.128-158.
- Glasdam, S. & Stjernswärd, S. (2020) Information about the COVID-19 pandemic – A thematic analysis of different ways of perceiving true and untrue information. *Social Sciences & Humanities Open*, *2*(1), pp. 1–10. (2020) doi: 10.1016/j.ssaho.2020.100090, E.T.19.12.2021.
- Hurriyet Gazetesi, (2000, January 10th) *Mossad'tan Esat'a idrar tahlili*, available at: https://www.hurriyet.com.tr/dunya/mossadtan-esata-idrar-tahlili-39124970, access on, 16.10.2022.
- Ikeda, S. (2020) As Global Pandemic Unfolds, Elite Hackers Attempt Cyber Espionage Against the WHO, available at: https://www.cpomagazine.com/cyber-security/as-global-pandemic-unfolds-elite-hackers-attempt-cyber-espionage-against-the-who/, access on 02.11.2022.

- Kaufman, DC. (2001) *Medical Intelligence: A Theater Engagement Tool,* U.S. Army War College, Pennsylvania, p.iii, available at: https://www.hsdl.org/?view&did=480818, access on 14.10.2022.
- Kaçakçılık İstihbarat Koordinasyon Kurulunun Toplanma, Çalışma Esas ve Usulleri Hakkında Yönetmelik, 4.11.1987, Resmî Gazete, 19624, available at: https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=8054&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5, access on 22.09.2022.
- Kocabaş, G. (2022, June 6th) Şeytanın aklına gelmeyecek sızma girişimi! Uzmanlar uyardı, Milliyet Gazetesi, available at https://www.milliyet.com.tr/gundem/hedeflerinde-kalbimiz-var-seytanin-aklima-gelmeyecek-sizma-girisimi-6704151, adresinden erişildi. access on, 22.09.2022.
- Lentzos, F. (2018, November 19th) *The Russian disinformation attack that poses a biological danger*. Bulletin of the Atomic Scientists, available at: https://thebulletin.org/2018/11/the-russian-https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/, Accessed on, 25.11.2022
- Maliye Bakanlığı Gelirler Genel Müdürlüğü, Vergi İstihbarat Uzmanlığı Görev, Yetki, Çalışma ve Atama Yönetmeliği, 10.01.1997, Resmi Gazete, 22873, available at: https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=4648&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5, access on 18.10.2022.
- Masood, I., Wang, Y., Daud, A., Aljohani, N.R., & Dawood, H. (2018) Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure, *Hindawi Wireless Communications and Mobile Computing*, Volume Article ID 2143897, pp.1-24, https://doi.org/10.1155/ 2018/2143897, access on 19.10.2022.
- Mcdermott, R. (2007) The Use and Abuse of Medical Intelligence. *Intelligence and National Security*, *22*(4), pp.491-520, https://doi.org/10.1080/02684520701640472, Access on, 21.11.2022
- Milliyet Gazetesi, (2013, September, 24th) available at: https://www.milliyet.com.tr/gundem/ suriyelilerden-yayilan-bu-hastalik-turkiyeyi-sariyor-1767683, Access on, 16.11.2022.
- MİT Başkanlığı (2021) available at: https://www.mit.gov.tr/isth-olusum.html, access on 20.09.2022.
- NATO, (1999) AJP-4.10 Allied…a.g.y., p. 32-33; “*Medical Intelligence*”, available at: http://www.scribd. com/ doc/73607402/t%C4%B1bbi-istihbarat, access on 19.11.2022.

- Özcan, N.A. (2020, April 14th), Korona Sürprizi ve tıbbi İstihbarat, Milliyet Gazetesi, 14.04.2020, available at: https://www.milliyet.com.tr/yazarlar/nihat-ali-ozcan/korona-surprizi-ve-tibbi-istihbarat-6188097, Access on, 27.09.2022.
- Özdağ, Ü. (2002) “Stratejik İstihbarat”. *Avrasya Dosyası Dergisi*. 8(2), 2002: 109-149.
- Özdağ, Ü. (2011) İstihbarat Teorisi, (5.bs), Kripto Yayınları, Ankara, pp.17-124.
- Savunma, Güvenlik ve İstihbarat İle İlgili Kamu İdarelerine Ait Devlet Mallarının Denetimi Sonucunda Hazırlanan Raporların Kamuoyuna Duyurulmasına İlişkin Yönetmelik, 15.08.2012 Resmî Gazete, 28385, available at: https://www.resmigazete.gov.tr/eskiler/2012/08/ 20120815-2.htm, access on 19.10.2022.
- Seren, M. (2020, May 13th) Kovid-19 krizi ve istihbarat kurumları*,* Habertürk Gazetesi, available at: https://www.haberturk.com/analiz-kovid-19-krizi-ve-istihbarat-kurumlari-2677923, access on 18.11.2022.
- Shaban-Nejad, A. Michalowski, M and Buckeridge, DL. (2018) Health intelligence: how artificial intelligence transforms population and personalized health, *npj Digital Medicine*, pp.1:53, available at: https://doi:10.1038/s41746-018-0058-9, access on 26.10.2022.
- Smith, CA. (1996) Plague in the Ancient World: A Study from Thucydides to Justinian*,* available at: http://people.loyno.edu/~history/journal/1996-7/Smith.html, access on 29.09.2022.
- Tharoor I, (2021) The Black Death, time.com, available at: http://content.time.com/time/ specials/packages/article/0,28804,2027479_2027486_2027547,00.html, access on 29.09.2022.
- Tiryaki, E. ve Özdal, B, (2020) Açık Kaynak İstihbaratında Sosyal Medyanın Rolünün Analizi, *ARHUSS*, 3(2), pp.267-296, Access on, 20.01.2022.
- Tümer, D.Ö, (2020, April 13th) Medikal istihbaratın önemi ve en verimli dönemi, Milliyet Gazetesi, available at: https://www.milliyet.com.tr/yazarlar/didem-ozel-tumer/medikal-istihbaratin-onemi-ve-en-verimli-donemi-6187322, access on 20.12.2022.
- Türk Silahlı Kuvvetleri, Millî İstihbarat Teşkilâtı, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı Taşınır Mal Yönetmeliği, Resmi Gazete, 10.12.2003, 27652, available at: https://www.mevzuat.gov.tr/MevzuatMetin/3.5.2010616. pdf, access on 12.08.2022.
- US Army (2008) 42 U.S.C. 7383e - *Annual report by the President on espionage by the People's Republic of China*, p. 6, available at: https://www.govin-

fo.gov/app/details/USCODE-2008-title42/USCODE-2008-title42-chap84-subchapXV-sec7383e/context, access on 21.09.2021.
- Ünlü, F. (2020, May 23th) Medikal İstihbaratın Esasları, Sabah Gazetesi, available at: https://www.sabah.com.tr/yazarlar/ cumartesi/ferhat-unlu/2020/05/23/medikal-istihbaratin-esaslari, access on 23.05.2022.
- Valdivia-Granda, W.A. (2021) Known and Unknown Transboundary Infectious Diseases as Hybrid Threats, *Front Public Health*, 2021; 9: 668062, doi: 10.3389/fpubh.2021.668062.
- Valdivia-Granda, W.A. (2020) Richt JA, What We Need to Consider During and After the SARS-CoV-2 Pandemic, *Vector-Borne And Zoonotic Diseases*, Volume 20, Number 7, Mary Ann Liebert, Inc., pp.477-483, DOI: 10.1089/vbz.2020.2652.
- WHO (2003) *The World Health Report 2003*. WHO, available at: http://who.int/whr/2003/en/whr03_en.pdf, access on 20.07.2022.
- Waller, A.E., Scholer, M., Ising, A.I., & Travers, D.A., (2011) Chapter 3: Using Emergency Department Data For Biosurveillance: The North Carolina Experience. In; Zeng D., Castillo-Chavez C., Chen H., Lober WB, Thurmond M. (Eds.) *Infectious Disease Informatics and Biosurveillance*. New York: Dordrecht, Heidelberg, London, Springer, pp 45–66. DOI 10.1007/978-1-4419-6892-0, ,
- Weir, L. and Mykhalovskiy, E. (2010) 5 A World on Alert: Emergency Vigilance in Global Biopolitics, *Global Public Health Vigilance: Creating a World on Alert*. New York, NY: Routledge.
- Yan, P. Chen, H. ve Zeng, D. Syndromic Surveillance Data Sources And Collection Strategies (2010) *Infectious Disease Informatics*, Springer Science+Business Media, LLC 2010, New York, pp. 33-48.
- Yılmaz, S. (2007) Küreselleşme ve Güvenlik, *21.Yüzyılda Güvenlik ve İstihbarat*, Milenyum Yayınları, İstanbul, pp. 33-54.

Valentin CHIRIȚA, PhD [*]
Associate Professor,
Police Colonel,
“Stefan cel Mare”
Academy of the Ministry of Internal Affairs
Republic of Moldova

Review paper
Received: 13 February
Accepted: 9 May 2023
UDK: 343.59(4:478)
https://doi.org/10.47152/rkkp.61.1.7

Ana-Maria CHEPESTRU, PhD student [**]
“Stefan cel Mare” Academy of the Ministry of Internal Affairs
Republic of Moldova
Main officer of the Political directorate
in the field of public order and security, fighting crime
of the Ministry of Internal Affairs

THE OFFENCE OF MASS DISORDER IN THE CRIMINAL LAWS OF SOME EUROPEAN STATES

The legal system of each state consists of a wide range of legal rules. Thus, national security and legal order are a high priority for each nation and manifest themselves distinctly within any state. In the Republic of Moldova, the mentioned social value is protected both: the contravention and by the criminal law. This paper aims to make a study of the crime of mass disorder in the Republic of Moldova in comparison with European countries. The comparative analysis of the crime will contribute to the examination of European legal norms and to the research of the possibility of including some provisions in the legal framework of the Republic of

[*] email: valentin-chirita@yandex.ru
[**] email: anamaria.1996@mail.ru

Moldova. Similarly, the good practices of European countries will be taken into account through the elements of comparative criminal law.

Keywords: state, public order, security, nation, social value, criminal law

1. Introduction

In the context of the accession of the Republic of Moldova to the European Union, it is mentioned that the analysis of the criminal law of the Republic of Moldova by comparing it with the criminal law of the European states will ensure the perception of specific legal norms that refer to public order and security. Namely, the parallelism between two or more criminal laws ensures a prolific analysis of national legal rules, institutions, and legal systems based on comparison methods. Hence, the importance of knowing the comparative criminal law field is highlighted, as it makes it possible to highlight a legal universalism obtained over time and the broad comprehensibility of several foreign legal systems. It is worth noting that the compared criminal law includes a set of information, which needs to be thoroughly processed in the light of the laws of each state separately.

Therefore, taking into account the topic addressed in this study, it is noted that the analysis of the mass disorder offence, in the light of comparative criminal law, will ensure the uniform and correct interpretation of legal norms, the appearance of the main similarities and differences between illegal acts similar to mass disorders incriminated in other states, as well as contributing to the improvement of the criminal legislation of the Republic of Moldova.

The analysis of the criminal legislation of foreign countries allows, firstly, to reveal the particularities of the legislative regulation of the crime component and, secondly, to assess the possibility of borrowing them for criminal domestic legislation. Foreign experience in the regulation of criminal law allows a better understanding of the importance of the social importance of criminal law. Study experience opens up new horizons and requires a better knowledge of their own legislation because the specific features of the law are highlighted in the analysis comparative analysis with other systems (Puica, 2019: 20).

2. Applied methods and materials

In the analysis of the mentioned subject, the comparative analysis method was used as the main research method. This is a universal process, involving the identification of similarities and differences between two or more aspects and the drawing of general conclusions based on them. Other research methods, such as: systematic, logical analysis, logical interpretation, etc. were also used. At the same time, it is communicated that the scientific grounds of the research are the analysis of the studies on the topic included in the manuals, scientific articles, collections of conference materials, etc. Simultaneously, this paper includes extensive investigations of the criminal laws of the states subject to comparative analysis.

3. Results obtained and discussions

Comparative criminal law is a field of the science of criminal law that has the subject of study of the rules and institutions legal systems belonging to different systems of criminal law, in order to understand their meaning and content and the differences between these rules and institutions. From this perspective, we have considered it appropriate to study the scientific approach dedicated to the offence of copyright infringement and related rights through the prism of the elements of comparative criminal law (Cojocaru, Cazacicov, 2015 :19).

Public security is a complicated social category for which no single conception has not yet been developed. Public security means a system of rules that ensures the protection of the most important values of persons, material and spiritual values of society, the authority of official power, as well as the sovereignty and territorial inviolability of the country. Public order is a system of rules of social coexistence, the normal functioning of state or public bodies, as well as social relations between citizens in all areas of social activity, accepted by society (Chiriță, 2021: 35).

The notion of national security reflects the qualitative state of society and the state, capable of ensuring safe and stable living conditions and the existence of its citizens, guaranteeing the protection of the rights and freedoms of every member of society, creating the premises and conditions for the stable development of the country. This means ensuring the defence of its values against internal and external dangers, of the basic material, intellectual and moral resources of existence, the order constitutional order and state sovereignty, independence, and

territorial integrity. In a different but similar vein, some authors consider that state security refers to the protection of sovereignty, independence, and integrity territorial, its constitutional system, its economic, technical, scientific, and defensive potential, the legitimate rights and freedoms of the individual against the informative and subversive activity of special services and foreign organizations, against criminal attacks by particular groups or individuals (Rotaru, 2018: 415).

The security of the state and society, as well as the safety of the individual, constitutes fundamental social values, whose existence and unrestricted realisation depend, on the normal course of the activity of the rule of law in the performance of its tasks and functions. The rigorous regulation of social relations, the establishment of the whole of life on the firm foundations of legality, the rule of law and discipline, is a natural, with the enlargement of the European Union and the increasing migration trends, the issue of public order and public safety in Europe is of the utmost topicality, as the following are increasingly evident the concerns of decision-makers and citizens alike, who are finding it increasingly difficult to accept the climate of insecurity. That is why, the focus of state and public authorities' concerns must be, at all times and consistently, public order and the safety of citizens, as major benchmarks that condition the proper functioning of all state institutions (Robea, 2015: 147).

Art. 285 of the Criminal Code of the Republic of Moldova provides for criminal liability for three offenses in the standard version, i.e. for three different offenses. Paragraphs 2 and 3 of art. 285 doesn't contain aggravating circumstances in relation to the rule in para. (1) art.285, but separate offences. This means that all three offenses referred to in this article can enter the competition or, it is not excluded that one and the same person will organize, instigate or even actively participate in mass disorders (Copeţchi, 2020: 27).

Thus, in art. 285 para. (1) is incriminated the action of organizing or conducting mass disorders, accompanied by the application of violence against persons, pogroms, fires, destruction of goods, the application of the firearm or other objects used as weapons, as well as the opposition of violent or armed resistance to the representatives of the authorities, which is punishable by imprisonment from 4 to 8 years. Paragraph (2) of the same article regulates the action of active participation in the committing of the actions referred to by paragraph (1), which is punishable by imprisonment from 3 to 7 years, and by paragraph (3) the calls for active violent disobedience to the legitimate requirements of the representatives of the authorities and to mass disturbances, as well as to the committing of acts of violence against persons, which are punishable by a fine in the amount of 550 to 850 conventional units or by unpaid work in the benefit of the community

from 180 to 240 hours, or by imprisonment up to 2 years (Codul penal al Republicii Moldova, 2002).

In light of the above, a broad and customized analysis of the illegal acts similar to the offence of mass disorder, which are incriminated in the criminal laws of foreign states, as follows, will be carried out.

3.1. Romania

The criminal legislation of Romania regulates the protection of social cohabitation regarding public order and peace seriously approached in Title VIII Chapter I of the Special Part of the Criminal Code of Romania of July 17, 2009. Unlike the offense provided by art. 285 of the Criminal Code of the Republic of Moldova, in the Romanian criminal law, art. 371, the disturbance of the order of public peace is criminalized, which is punishable by imprisonment from 3 months to 2 years or by a fine, which constitutes the act of the person who, in public, by violence committed against persons or property, or by threats or serious harm to the dignity of persons, disturbs public order and tranquility (Codul penal al României, 2009). From this is inferred an essential difference both between the titles of the offences and between their objective side, which at first glance may seem similar.

Making a tangent to art. 285 para. (3) of the Criminal Code of the Republic of Moldova, which is materialized by calls for active violent disobedience to the legitimate requirements of the representatives of the authorities and to mass disturbances, as well as to the perpetration of violence against persons, it is noted that the Criminal Code of Romania provides in art. 368 – Public incitement, which represents the act of urging the public, verbally, in writing, or by any other means, to commit offence and shall be punished with imprisonment from 3 months to 3 years or with a fine, without exceeding the punishment provided by law for the offense that was instigated (Codul penal al României, 2009).

Subsidiary, considerable differences are noted regarding the punishments for the alleged facts. A gap is manifested by the fact that the Moldovan legislation clearly and concretely establishes the amount of the fine, but in the Romanian one the amount of the fine remains to be interpretable, according to the inner conviction of the competent organizations. At the same time, there are disproportionalities in the case of the term of the sanction of deprivation of liberty, which varies depending on the illegality committed by the perpetrator.

3.2. Poland

In the Polish Criminal Code, offences against public order are found in Chapter XXXII. Although the chapters of the mentioned code have concrete titles and are structured according to the attention objects, it is noted that the articles do not contain titles. Therefore, it is pointed out that paragraph 1 of art. 254 of the aforementioned Code expressly states that the person who actively participates in a meeting, knowing that the participants commit by common force an attack with violence against a person or an asset is sanctioned with the penalty of imprisonment of up to 3 years. Similarly, paragraph 2 of the same article provides that if the result of the violent attack is the death of a person or serious damage to his/ her health, the participant in the meeting referred to in paragraph 1 shall be punished with the imprisonment of a 3 months to 5 years duration (The criminal code of Poland).

The exposed deed can be easily likened to the action of active participation in committing mass disorders regulated by art. 285 paragraph (2) of the Moldovan Criminal Code. However, the Polish lawgiver provides for the sanctioning of the deed with the sentence of deprivation of liberty up to 3 years, and in case of death or serious damage to the health of the person – with a maximum of 5 years, but the Moldovan one - with imprisonment from 3 to 7 years, setting the term of 7 years as the maximum limit. Hence, it is pointed out that in the Republic of Moldova, active participation in mass disturbances is punished more harshly compared to Poland.

In this respect, it is relevant art. 255 paragraph 2 of the Polish Criminal Code, which states that the person who publicly instigates the commission of a offence, is punished with imprisonment of up to 3 years (Toader, 2018: 3494). This legal norm can be analyzed in conjunction with art. 285 paragraph (3) of the Moldovan Criminal Code. By analogy, calls for active violent disobedience to the legitimate demands of the representatives of the authorities and to mass disturbances, as well as to the perpetration of acts of violence against persons are materialized by addressing calls to the committing of such illegalities.

In the specialized literature, addressing calls for the mass disorder is perceived as a qualified instigation in relation to the illegal acts mentioned in 285 para. (2) of the Moldovan Criminal Code and is assimilated to the offence perpetrator. In this context, addressing calls to commit acts of violence against persons implies the determination of other persons to undertake illegal acts. However, not every type of incitement to violence constitutes the composition of an exposed offence (Brînza, Stati, 2015: 586).

As a result of the research into the composition of the offence, there was found a similarity between the legal norms concerned, a fact existing in the action itself to incite the public to commit clandestine activities, in the case of mass disturbances. At the same time, it is specified on some differences related to the type and term of the sanction in the case of the mentioned deed, in the Republic of Moldova the deed is punished both with a fine and with deprivation of liberty for a period of up to 2 years, and in Poland only with deprivation of liberty for up to 3 years.

3.3. Germany

In the German Criminal Code, the offence addressed is to be found in Section VII “Offences against public policy”, articles 125, 125a, and 126. The classic variant of the offense is regulated by art. 125 “Disturbance of public order”. Thus, paragraph (1) of the aforementioned paragraph stipulates that the person who participates as an author or participant in acts of violence against people or property or in threats of violence against people committed within a group organized in a way that endangers public safety or the person who urges a group of persons to commit such acts shall be punished with imprisonment of up to 3 years or a fine. Paragraph (2) of the same article provides that whereas article 113 provides for a penalty for the actions referred to in para. (1) and (2), the provisions of art. 113 (3) and (4) shall apply having regard to the corresponding modifications in meaning. This shall also apply in the cases provided for by art. 114 if the act exercised by virtue of the work duties is an act within the meaning of the provisions of art. 113 para. (1).

At the same time, it is worth mentioning that art. 125a of the German Criminal Code “Disruption of public order with particularly serious consequences” exposes an aggravating form of the offence concerned supra. Respectively, in the particularly serious cases provided for by art. 125 para. (1), the punishment is imprisonment from 6 months to 10 years. A particularly serious case is usually the case where the perpetrator: 1. carries a firearm, 2. carries another kind of weapon or other dangerous instrument, 3. by an act of violence brings another person in danger of death or serious injury to his health, 4. plunders or causes considerable damage to property that does not belong to him (The criminal code of Germany).

In such circumstances, it is noted that the title of the offense used by the German lawmaker differs from that used in the legislation of the Republic of

Moldova. However, it is inferred that the German legislature provides directly for criminal liability for the perpetrator and the participant in acts of mass violence, but does not regulate criminal liability for the organizer, but directly for the perpetrator. Similarly, the German legislature regulates the liability for the exhortation of a group of persons to commit the disturbance of the peace, and such an action is provided in art. 285 para. (3) of the Criminal Code of the Republic of Moldova in the form of calls for active violent disobedience to the legitimate requirements of the representatives of the authorities and to mass disturbances, as well as to the perpetration of violence against persons.

It is relevant that in Germany an aggravating circumstance is also regulated for disturbances of public peace, for which a much harsher punishment is regulated (up to 10 years in prison) compared to the type of offense, for which a sentence of imprisonment of up to 3 years or a fine is provided. Therefore, it is communicated that in the Republic of Moldova, the criminal liability for committing mass disturbances is much more severe than in Germany, with the period of imprisonment being practically assimilated to the aggravating form of disturbances of public order committed in Germany.

3.4. France

In the French Criminal Code, the punishment for disturbing the peace is found in Title III, Chapter I, Section 3 “About illicit manifestations and the participation in a public event or meeting”, more specifically in art. 431-9 which has no title, which in our opinion makes it difficult to identify the given fact among other similar facts.

According to the mentioned article, it is punished with 6 months imprisonment and a fine of 7 500 euros: 1. the organization of an event on the public road which has not been the subject of a prior declaration under the conditions established by the law; 2. the organization of an event on the public road which has been prohibited under the conditions established by the law; 3. the incomplete or inaccurate declaration likely to deceive on the object or conditions of the planned event. Similarly, the provisions of art. 431-10, according to which the participation in a manifestation or in a public meeting carrying a weapon is punishable by 3 years imprisonment and a fine of 45 000 euros (The criminal code of France).

Therefore, it is mentioned that the composition of the French offence is totally different from the Moldovan one and does not directly punish the actions of participation, organization, the conduct of mass disturbances, nor the call to active violent disobedience to the legitimate demands of the representatives of

authorities and to mass disturbances, as well as to the perpetration of acts of violence against persons. It punishes only the violation of procedural conditions in the process of organizing public manifestations, i.e. the lack of statements on public manifestations.

However, it is appropriate to highlight the art. 421-1 of the French Criminal Code, according to which they constitute acts of terrorism if they are intentionally related to an individual or collective activity aimed at seriously disturbing the public order by intimidation or terror. Simultaneously, art. 421-2-5 of the same Code establishes that directly provoking acts of terrorism or public incitement to such acts is punishable by 5 years imprisonment and a fine of 75 000 euros. The sentences are 7 years in prison and a fine of 100 000 euros if the deeds were committed through the use of an online public communication service. If the acts are committed by the written or audiovisual press or by online public communication, the particular provisions of the laws governing these matters shall apply as regards the determination of the persons responsible (The criminal code of France).

In view of the above, it is inferred that in France, namely, any action aimed at a serious disturbance of public order falls under the incidence of acts of terrorism. By making reference to the criminal legislation of the Republic of Moldova, it is communicated that the terrorist act is incriminated in art. 278 of the Criminal Code of the Republic of Moldova, which materializes through causing an explosion, a fire, or the commission of another act that creates the danger of causing death or injury to the bodily integrity or health, essential damage to property or the environment or other serious consequences, if this act is committed in order to intimidate the population of a state or part of it, to draw the attention of the society to the political, religious or other ideas of the perpetrator or to compel a state, an organization, a legal or natural person to commit or to refrain from any action, as well as the threat to commit such acts for the same purposes and shall be punished with imprisonment from 6 to 12 years (Codul penal al Republicii Moldova , 2002).

It is worth mentioning that in France, the punishment for disturbing the public order is quite severe in terms of the amount of the fine, which is very expensive compared to the Republic of Moldova. In part related to imprisonment, the legislation in France is also much harsher than in the Republic of Moldova.

3.5. Finland

From the earliest notations of the Finnish Criminal Code, an exhaustive list of notions of particular relevance is listed and explained. That is, it highlights the definition of revolts, which occurs when a group clearly intends to use violence

against a person or cause significant damage to a property, and a person actively participating in the group's actions, and in this context, the person does not comply with a legal order issued by a competent official to disperse, the person is convicted of revolt. In Chapter XVII, Section 2 of the said Code is expressly regulated that for the conduct of revolts, persons may be sanctioned with a fine or imprisonment for up to one year. Section 3 of the same Chapter provides for criminal liability for violent rebellion, which occurs when a group commits an offence referred to in Chapter 16, Section 1 and uses violence against a person or causes significant damage to a property, and a person that actively participates in the group's actions is sentenced for violent rebellion to a fine or imprisonment for a maximum of 2 years (The criminal code of Finland).

Just like in the case of art. 285 para. (1) of the Moldovan Criminal Code, the person leading the revolts in Finland, is also criminally liable, except it is based on a separate provision from the basic composition. Therefore, according to Section 4 “Lead a violent uprising”, a person who incites or leads a group referred to in Section 3 is sentenced for leading a violent uprising to a maximum of 4 years in prison.

In the same context, it is communicated that according to the Law on Public Order of the Republic of Finland (512/ 2003), a summary criminal fine may be imposed on persons who infringe public order, which, according to Chapter 2 (A) Section 8 of the Finnish Criminal Code, is a pecuniary penalty consisting of a fixed amount in euro, which is less severe than a fine (Toader, 2018: 1232).

It should be mentioned that the term of revolt used in the Finnish criminal legislation, as a meaning, is closer to the notion of mass disorders used in the criminal legislation of the Republic of Moldova. In this respect, analyzing the ideas of several Moldovan doctrines, it is inferred that the mass disorders depict a social event with a high degree of danger, which affects the normal evolution of the state. The causes of their occurrence may be multiple and of diverse nature, for example, the disagreement of the members of society with the actions and/ or inactions of the state representatives, the manifest and repeated violation of human rights and fundamental freedoms, the claim of necessary social needs on the part of citizens, the existence of unclarified antagonisms, which escalate in time and space, etc.

3.6. Spain

The Criminal Code of the Kingdom of Spain protects social values with regard to public policy in the content of Title XXII, Chapter III. With reference

to the topic addressed, it is communicated that in the nominated state, the punishment for the attack on public peace is found in art. 557 "Public disorder", which in paragraph 1 provides that persons who, acting in a group and for the purpose of attentive to public silence, shall be punished with the penalty of imprisonment from 6 months to 3 years shall be punished with the penalty of imprisonment, disturbs public order by causing injury to persons, causing damage to property, placing obstacles on public roads or access roads to them, thus endangering the movement on those roads or occupying installations or buildings, without prejudice to appropriate penalties which may be imposed on them, in accordance with other provisions of the Code concerned. Paragraph 2 of the same article states that the penalty higher in degree than those provided for in the preceding paragraph shall be applied to the perpetrators of the acts referred to in that paragraph, when they occurred during the performance of events or performances involving a large number of persons. With the same punishment will be punished persons who, inside the premises where these events take place, disturb the public order by behaviours that cause or are likely to cause a dangerous situation for some of the participants. In these cases, it will also be possible to apply the punishment of the prohibition to participate in events or performances of the same kind for a period of 3 years longer than the duration of the main punishment applied (The criminal code of Spain).

In contingency with what was reported, namely from the content of the offence composition, it is noted that the Spanish lawmaker, just like the Moldovan one, emphasizes the material legal object of the investigated offence, in both cases the priority being the physical body of the person and the movable and/ or immovable property. Another approximation between the offences concerned consists in their very title, in our view they are exposed by paronymy, being differentiated through a single phrase.

However, a difference is noted in the part related to the article structure, where the Criminal Code of the Republic of Moldova includes three standard type variants of the offence of mass disorder, and the Spanish Criminal Code contains in para. 1 the basic composition, and in para. 2, an aggravating circumstance thereof.

Also, it is highlighted that in the Republic of Moldova, the criminal punishment is harsher for the organization, leadership, and active participation in mass disturbances compared to Spain. On the other hand, in the Spanish Criminal Code, for the aggravation of the investigated offense, a complementary punishment is provided, namely the prohibition to participate in events or performances of the same type for a period of 3 years longer than the duration of the main

punishment applied, which is interpreted at the discretion of the bodies with competence in the field of investigating offences.

In connection with the public provocation action, it is noted that the Spanish Criminal Code does not make a materialization regarding the public incitement of persons to mass disorder, but in art. 18, para. (1) shall contain a general explanation indicating that there is incitement to commit an offence directly, by means of printouts, by broadcasting or by any other means that have a similar effect, which facilitates advertising, or in front of a group of persons.

3.7. Sweden

Among the first regulations in the Swedish Criminal Code, the notion of revolt is explained. art. 1 of Chapter 16 of the Swedish Criminal Code provides that if a lot of people disturb public order, manifesting the intention that, by joining forces, to protest against an authority or otherwise to provoke or prevent a certain measure and not to disperse at the order of authority, the instigators and leaders are punished for the revolt with imprisonment up to 4 years, and other participants in the activity of the crowd with a fine or imprisonment of up to 2 years. If the crowd disperses by order of authority, the instigators and leaders shall be punished for mutiny with a fine or imprisonment of up to 2 years. art. 2 of the same chapter stipulates that if a crowd, with the intention mentioned in art. 1, has joined forces against a person or property, is punishable, whether authority was present or not, for violent revolt, instigators and leaders with imprisonment of up to 10 years, and other participants in the activity of the crowd with a fine or imprisonment of up to 4 years (The Swedish Criminal Code).

At the same time, it is mentioned that the Moldovan criminal legislation omits to explain the notion of mass disturbances, while the Swedish legislation, just like the Finnish one, explains an exhaustive list of notions at the beginning of the Criminal Codes, including the term of revolt. This fact ensures the materialization of actions that can be qualified as mass disorders and facilitates the activity of competent bodies in the investigation of such facts.

As in the Republic of Moldova, the same article in Sweden imposes criminal liability on instigators, leaders, and participants in mass disturbances, but through different paragraphs. In the Republic of Moldova, for the leaders of the mass disorders, there is a prison sentence of 8 to 15 years, and for the instigators a fine in the amount of 550 to 850 conventional units or unpaid work for the benefit of the community from 180 to 240 hours, or imprisonment up to 2 years, while in Sweden for these categories of persons - imprisonment up to 4 years. For

active participation in mass disturbances, the Moldovan criminal legislation provides for a prison sentence of 3 to 7 years, while the Swedish one – a fine or imprisonment of up to 2 years. It is relevant to mention that the Swedish Criminal Code does not regulate the minimum and maximum limits of the fine as stipulated in the Moldovan Criminal Code.

Art. 2 of Chapter 16 of the Swedish Criminal Code provides for an aggravating form of revolts, which is punished more severely compared to the classic form of the offence. Basically, it is inferred that in the Republic of Moldova, the punishments for mass disturbances are similar in size to the punishments stipulated for committing revolts in Sweden under aggravating circumstances.

3.8. Denmark

The Danish Criminal Code criminalizes offences against public order and peace in Chapter 15. Thus, in art. 133 para. (1) it is mentioned that the person who urges the crowd to violence or to threaten violence on the person or on the property is punished by a fine or by imprisonment of up to 3 years. Paragraph (2) of the same article provides that with the same punishment shall be sanctioned the persons who, within a crowd, for any purpose pursued that day, act as leaders, as well as any participant who does not comply with the order of the authorities to disperse. Similarly, para. (3) prescribes that if in such a crowd an offense is committed in connection with its purpose, the instigators or the leaders of the crowd are sanctioned with the punishment provided by law for that offense.

It is appropriate to specify an attenuating circumstance of the basic offence, namely art. 134 according to which, the person who participated in such a crowd and who, knowing that a scattering order was legally issued, does not comply, is punished with a fine or imprisonment of up to 3 months.

At the same time, the provisions of art. 134a, according to which the participants in brawls or other serious disturbances of public order, if they acted following an agreement or together, are sanctioned with imprisonment of up to 1 year and 6 months (The criminal code of Denmark).

A unique provision that we have identified in the Denmark criminal law, which we have not observed in the criminal law of any state addressed in this study, is the stipulation of the punishment for the fact that during some meetings, gatherings, marches or other public demonstrations, the person has his/ her face completely or partially covered by a face guard, mask, painting or something similar, so as to prevent his/ her identification. Respectively, for such an act, the person may be punished with a fine or imprisonment of up to 6 months according

to art. 134b of the Denmark Criminal Code. However, para. 3 of that article also provides for an exception to the rule mentioned above, namely that the prohibitions in question do not apply if the objects serve to cover themselves with a view to protecting them against weather or other legitimate purposes.

Just like in the Republic of Moldova, Denmark regulates the imprisonment of organizers, leaders, and direct participants in mass disturbances, and compared to the Republic of Moldova, the punishment is kinder. Similarly, the aggravating and mitigating circumstances of the mass disturbances are regulated in Denmark, while in the Republic of Moldova, criminal liability is provided for the classic type offence, without mitigating and aggravating.

3.9. Greece

In the starting point of the Greek Criminal Code, namely in the notes of the Special Part, the notion of inciting citizens to acts of violence or discord is explained as follows: the person who publicly in any way provokes or incites citizens to acts of violence between them or to mutual discord and thus disturbs the public peace is punished by imprisonment unless a more serious punishment is imposed according to other provisions.

Disturbance of the peace is incriminated in the Special Part, in Chapter VI art. 189. Thus, paragraph 1 states that the act of the person taking part in a public meeting consisting of several natural persons who, in mass, commit acts of violence against persons or things or illegally enter foreign houses, dwellings or other buildings is punishable by imprisonment of up to two years. Paragraph 2 expressly states that the act of instigators and persons who committed acts of violence is punishable by imprisonment for at least three months, and paragraph 3 regulates that these punishments apply unless the act is punished with more severe punishment by other special provisions (Toader, 2018: 2029-2030).

In conjunction with art. 285 of the Criminal Code of the Republic of Moldova, it is specified that the basic component of the given offense is stipulated in paragraph 1. At paragraph 2, an attenuating circumstance is observed for the instigators of such acts, the punishment being much lower than that indicated for the offenders, and paragraph 3 provides only a mention consisting of a determination for information, without incriminating another related deed.

Another correlated deed is found in art. 190 of the code concerned, which outlines that the act of the person who, with the threat that offences or crimes will be committed, causes anxiety or fear to the citizens is punished with imprisonment of up to 2 years. It should be mentioned that the Moldovan criminal legislation

does not include such a regulation but only offers the possibility to legally frame the preparation and attempt of mass disorders. Respectively, to the qualification of such facts, art. 285 of the Criminal Code of the Republic of Moldova will be connected with art. 26 (preparation of the offense) or, as the case may be, with art. 27 (attempted offense) of the same code.

Although, art. 192 of the Greek Criminal Code does not have a concrete title, it states that the act of the person who, in any public way, provokes or incites the citizens to acts of violence between them or to mutual hatred and thus disturbs the public peace, is punishable by imprisonment for up to 2 years, unless the act is punished with more severe punishment by other special provisions. Similarly, it is reported that by analyzing the Greek Criminal Code in conjunction with the Swedish Criminal Code, a similarity can be found, in the sense that the titles of the articles are missing in both codes.

In other news, it is reported that in Greece the punishments for disturbing the public peace are kinder than those stipulated in the Criminal Code of the Republic of Moldova. Similarly, there is a big difference between the offence component of the mass disturbances stated in the Moldovan criminal legislation and the disturbance of the public peace regulated in the Greek one.

4. Conclusions

In the process of examining the subject at hand, we have investigated the criminal legislation of various states. In addition to the criminal legislation investigated in this paper, we have also explored other European criminal legislation and found that in most of them, the offence of mass disorder is found under various titles. For example, "common state disorder" is used in Cyprus, "violation of public order" is used in Estonia and Lithuania, "disturbance of the peace" is used in Germany, "disorderly conduct" is used in Slovakia, etc.

By virtue of the above, it is communicated that only in art. 285 of the Criminal Code of the Republic of Moldova identifies three type variants of the offence of mass disorder, each constituting a separate offence. In the other states, actions that violate public order and security can be combined, as in the Republic of Moldova, but can also be reflected in separate articles, such as, for example, in the case of Romania, which provides for public provocation in a separate article. At the same time, in some states examined in this study, there are mitigating and aggravating circumstances of the mass disturbances, while in the Criminal Code of the Republic of Moldova, such circumstances are not stipulated.

Similarly, using the criterion of likeness, it is found that the title of the offense “Disturbance of public order and peace” exposed in the analyzed foreign criminal laws is identical to the title of the contravention “Disturbance of peace”, stated in art. 357 of the Contravention Code of the Republic of Moldova, however, they cannot be likened in any way in the part related to the degree of prejudice of illicit actions and the measure of attention to the values and social relations protected by the legislation.

Another quite significant epilogue is the fact that neither in the Criminal Code of the Republic of Moldova nor in any other Criminal Code of any foreign state examined in the paper, there are no regulations regarding the type of violence applied in the context of mass disturbances. In this regard, it is communicated that the normative framework of the Republic of Moldova recognizes two types of violence: non-hazardous and dangerous for the life or health of the person.

As non-hazardous violence to the life or health of the person, minor injuries are considered. Violence that is dangerous to the life or health of the person is considered as violence that has resulted in average or slight injury to the integrity of the body or health or which, although it has not caused these consequences, involves at the time of its application, due to the method of operation, a real danger to life and health.

As an alternative, the committing of the actions referred to in art. 285 of the Criminal Code of the Republic of Moldova, involving either non-hazardous violence or dangerous violence for the life and health of the person. But, based on the severity of the bodily injuries, obscurities may occur, and the criminal nature of the harmful act may be overlapped with the contravention and vice versa. This lack of legislation can obviously generate interpretations regarding the type of violence and even errors in the process of the legal classification of the deed. Therefore, there is a risk that the activity of law enforcement bodies with competence in the field of investigating the offence will be difficult and stalled for a long time.

References

- Brînza, S, & Stati, V. (2015). *Tratat de derpet penal: Partea Specială, vol. II.* Chişinău: Tipografia Centrală
- Chiriţa, V. (2021) *Infracţiunea de luare de ostatici: Studiu monografic. Ediţie revizuită şi adăugită*. Chişinău. ISBN 978-9975-121-80-4
- Cojocaru, R, Cazacicov, A. (2015). Elemente de drept penal comparat privind infracţiunea de încălcare a dreptului de autor şi a drepturilor conexe. *Anale*

ştiinţifice ale Academiei „Ştefan cel Mare” a MAI al RM: ştiinţe juridice, 15(1), 18-26.
- Copeţchi, S. (2020). Infracțiunile de dezordini în masă (art. 285 CP RM): Noțiune, analiză, delimitare de fapte penale similare. *Revista Procuraturii Republicii Moldova,* no. 6, p. 27-36.
- Puica, V. (2019). Elemente de drept penal comparat privind infracţiunea de exces de putere sau depăşire a atribuţiilor de serviciu. *Legea şi Viaţa*, *11*(335), pp. 19-24. ISSN 2587-4365.
- Robea, M. (2015). Coraportul dintre noţiunile de ordine juridică, ordine de drept şi ordine publică. *Studii Juridice Universitare*, 1-2, pp. 146-154. ISSN 1857-4122.
- Rotaru, R. (2018) Dezordinile în masă. Măsuri juridice de profilaxie. *Criminalitatea transfrontalieră şi transnaţională: tendinţe şi forme actuale de manifestare, probleme de prevenire şi combatere* (pp. 414-420). Chişinău. ISBN 978-9975-121-48-4.
- Toader, T. (2018). *Codurile penale ale Statelor Uniunii Europene.* Bucharest: C. H. Beck Publishing House.
- Codul penal al Republicii Moldova nr.985/2002 (republished in the Official Monitor of the Republic of Moldova, 2009, no.72-74, art.195);
- Codul penal al României din 17 iulie 2009, adoptat prin Legea no. 286/2009 published in the Official Monitor no. 510 of July 24, 2009, accessed at: https://legislatie.just.ro/Public/DetaliiDocumentAfis/223635, at 24.11.2022;
- The Criminal Code of Denmark, translated into Romanian, accessed at https://codexpenal.just.ro/laws/Cod-Penal-Danemarca-RO.html , at 30.11.2022
- The Criminal Code of France, translated into Romanian, accessed at https://codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html, at 29.11.2022;
- The Criminal Code of Finland, translated into Romanian, accessed at https://codexpenal.just.ro/laws/Cod-Penal-Finlanda-RO.html , at 29.11.2022;
- The Criminal Code of Poland, translated into Romanian, accessed at https://codexpenal.just.ro/laws/Cod-Penal-Polonia-RO.html, at 25.11.2022;
- The Criminal Code of Spain, translated into Romanian, accessed at https://codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html, at 30.11.2022;
- The Swedish Criminal Code, translated into Romanian, accessed at https://codexpenal.just.ro/laws/Cod-Penal-Suedia-RO.html, at 30.11.2022.

About the journal

The Journal of Criminology and Criminal Law is triannual, peer reviewed scientific journal with over 60 year long tradition, co-published by the Institute of Criminological and Sociological Research- Belgrade and the Serbian Association for Criminal Law Theory and Practice. According to the categorization of the Ministry of education, science and technological development the Journal is categorized as M51 (Prominent/outstanding journal of the national importance). The Journal includes articles in the field of criminal law, criminology, penology, victimology, juvenile delinquency and other sciences that study etiology, phenomenology, prevention and repression of crime. Moreover, the Journal is indexed in the prestigious global database HeinOnline.

Papers should be submitted via Journal website at https://rkkp.org.rs/

Technical instructions for authors

1. The article should not exceed 36,000 of characters (with spaces). The authors should use Times New Roman font size 12.

2. The first page should include: **the title of the paper**, **the name and surname of the author**, **abstract** (up to 150 words) and **4-5 keywords**.
   2.1 Right after the surname of the author (on the first page) there should be a footnote with the name of the institution the author is employed at, the title of the author and E-mail address. In the event that the paper is written in collaboration with other authors, these data should be provided for each of the authors.

   Example: Jovan JOVANOVIĆ*

   2.2 The abstract should include a clearly stated subject, research goals and the main topics which will be covered in the paper.

3. Headings should be written in the following style:
   1. The title of the chapter (Times New Roman, 12, Bold)
   1.1. Subtitle 1 (Times New Roman, 12, Italic)
   1.1.1. Subtitle 2 (Times New Roman, 12, Regular)

   Example: 1. **Services Supporting Victims**
   1.1. *Categories of Users*
   1.1.1. Women and Children

---

* Dr Jovan Jovanović is assistant professor at the University in Belgrade. E-mail: jovan@primer.net

4. Authors should use the **Harvard Citation Style**. The quotation should be followed by the reference in the brackets containing author's surname, the year of publication and the page number.

   Example: (Stevanović, 2009: 152).

   If there are two or three authors, the surnames should be divided with a comma (example: Knežić, Savić, 2012).
   If there are more than three authors, there should be only first author's surname followed by the "et. al" (example: Hawley i dr., 2013).
   If two authors have the same surname, name initials should also be included (example: I. Stevanović, Z. Stevanović, 2015).
   When referencing a secondary source, the reference should include "according to" (example: Ćopić according to Nikolić-Ristanović, 2011).
   If a single reference contains several books or papers, they should be separated with a point comma. (example: Hannah-Moffat, 2005; Kemshall, 2002). In this case surnames of different authors should be in alphabetical order.

   4.1. Footnotes should include only following comments, articles of laws and official gazettes.

   4.2. Foreign names should be written with original spelling.

5. If the paper includes images or charts, they should also be referenced. For example (Chart 2).

   Captions should be written above the images or charts.
   Example: **Chart 1.** Gender structure of victimisation

6. It is obligatory to supply a list of references or **bibliography** at the end of the paper. It should include all the quoted references in the alphabetical order of surnames. An integral element of a bibliographic item is the **DOI (Digital object identifier) number**, for those references that are accompanied with this identifier. Doi number must be added at the end of the source. A bibliography unit should include:
   For books: author's surname, the name initial, the year of publication in the brackets, the title of the book (in italics), the location of publishing, the name of the publisher.
   Example: Milutinović, M. (1977) *Penology.* Belgrade: Savremena administracija.
   For book chapters: author's surname, the name initial, year of publication in the brackets, the name of the chapter, in: editor's name initial, editor's surname, eds. (in the brackets), the book title (in italics), the location of the publication, the name of the publisher, first and last page of the chapter.
   Example: Blagojević, M. (2013) Transnationalization and its Absence: The Balkan Semiperipheral Perspective on Masculinities. U: Hearn, J., Blagojević,

M. & Harrison, K. (ur.) *Transnational Men: Beyond, Between and Within the Nations*. New York: Routledge, str. 261-295.

For articles in journals: author's surname, name initial, year of publication in the brackets, the name of the article (in italics), volume (in italics), the number of the magazine in the brackets and first and last page number.

Example: Wright, R. F. (2017) Reinventing American prosecution systems. *Crime and Justice*, *46*(1), pp. 395-439. https://doi.org/10.1086/688463

For documents downloaded from the internet: web page, date of access.

Example: http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2, accessed on 5.10.2012

The name of the author and the title of the article can be written before copy/pasting the web page. In this case before the web address there should be added: "available at:"

For laws: the source or publication where the law was published should be added after the name of the law.

For reports from scientific conferences: surname, name initial, year in the brackets, the title, the title of the conference (in italics), page number in the book of abstracts in the brackets, the location of publication, publisher.

Example: Petrušić, N, & Stevanović, I. (2011) Legal Protection of Children in Serbia. *First Annual Conference of the Victimology Society of Serbia – The Rights of Victims and EU* (pp. 87-102). Belgrade: Victimology Society of Serbia.

For newspaper articles: surname, name initial, year of publication and the date in the brackets, the title of the article, the name of the newspaper, page number.

Example: Jovanović, A. (2012, December 5th) Plagiarising Scientific Papers, Blic, p. 5.

The author can also reference a web edition of a newspaper and in this case the reference should include "available at" followed by the web address and the access date.

Additional remark: The list of references must not contain units which are not quoted in the paper and must contain all the units which are quotes including laws, reports and web pages (web pages should be under the section *Online Sources* within bibliography).

7. **All papers are subject of a double-blind review as a necessary precondition for the positive decision on publishing.**

Papers may not be published or submitted for publishing anywhere else.

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

343

REVIJA za kriminologiju i krivično pravo = Journal of Criminology and Criminal Law / glavni i odgovorni urednik Božidar Banović. - Vol. 41, br. 1 (2003)-

– Beograd : Serbian Association for Criminal Law Theory and Practice: Institute of Criminological and Sociological Research, 2003- (Belgrade : Službeni glasnik). – 24 cm
Dostupno i na: http://www.iksi.ac.rs/revija.html.
– Tri puta godišnje. –

Glavni stvarni naslov na engl. jeziku od br. 1 (2018) Journal of Criminology and Criminal Law.
- Je nastavak: Jugoslovenska revija za kriminologiju i krivično pravo = ISSN 0022-6076
ISSN 1820-2969 = Revija za kriminologiju i krivično pravo
COBISS.SR-ID 116488460

ISSN 1820-2969

JOURNAL
OF CRIMINOLOGY AND CRIMINAL LAW