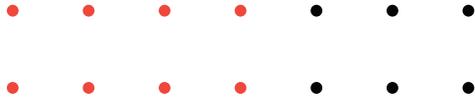
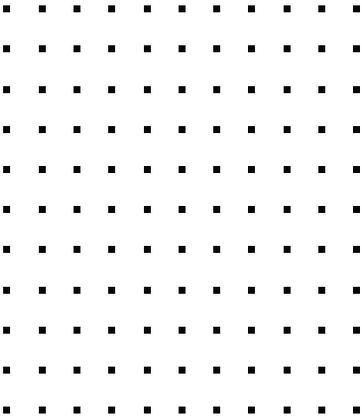


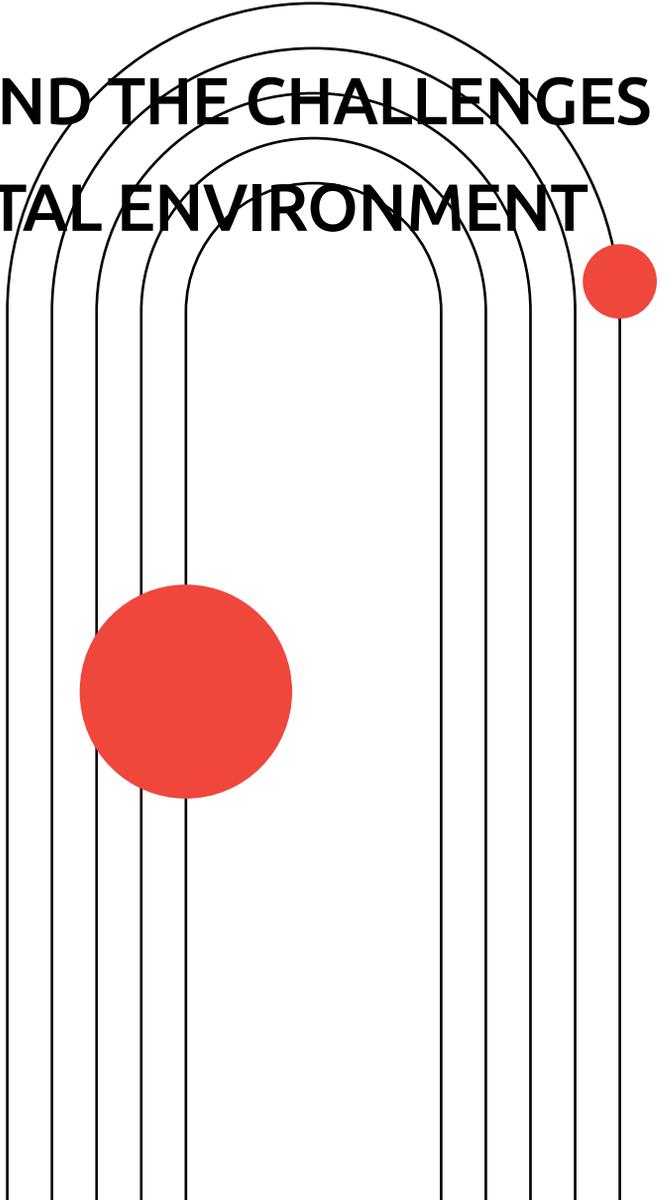
INSTITUTE OF CRIMINOLOGICAL AND SOCIOLOGICAL RESEARCH



CHILDREN AND THE CHALLENGES OF THE DIGITAL ENVIRONMENT

INTERNATIONAL SCIENTIFIC THEMATIC CONFERENCE

2022



International scientific thematic conference

Children and the Challenges of the Digital Environment

THEMATIC CONFERENCE PROCEEDINGS
OF INTERNATIONAL SIGNIFICANCE

Palić, 16-17 June 2022

Institute of Criminological and Sociological Research
Serbia, 2022

Publisher
Institute of Criminological and Sociological Research
Belgrade, Gračanička 18

For Publisher
Ivana Stevanović, PhD
Director of the Institute of Criminological and Sociological Research

Editors
Ivana Stevanović, PhD
Milica Kolaković - Bojović, PhD

Reviewers
Milan Škulić, PhD
Full Professor, Faculty of Law, University of Belgrade and Judge
of the Constitution of Court of Serbia, Republic of Serbia

Ivana Milas Klarić, PhD
Associate Professor, Faculty of Law, University of Zagreb, Republic of Croatia

Angelina Stanojoska, PhD
Associate Professor, Law Faculty, University “St. Kliment Ohridski” – Bitola,
Republic of North Macedonia

Prepress
Tatjana Zlatanović

Cover design
Ana Batrićević, PhD

Print
Pekograf d.o.o.

Impression
300 copies

The International Scientific Conference was supported by
THE MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGICAL
DEVELOPMENT SERBIA

INTERNATIONAL SCIENTIFIC CONFERENCE
CHILDREN AND THE CHALLENGES OF
THE DIGITAL ENVIRONMENT

PROGRAMME COMMITTEE

Vid Jakulin, PhD, Faculty of Law, University of Ljubljana, Slovenia

Elizabeta Ivičević Karas, PhD, Faculty of Law, University of Zagreb, Croatia

Đorđe Ignjatović, PhD, University of Belgrade Faculty of Law, Serbia

Academician, Vlado Kambovski, PhD, Macedonian Academy of Sciences and Arts, North Macedonia

Aleksandar Jugović, PhD, Faculty of Special Education and Rehabilitation, University of Belgrade, Serbia

Dalibor Petrović, PhD, University of Belgrade, Faculty of Philosophy, Department of Sociology, Serbia

Academician, Miodrag Simović, PhD, University of Banja Luka, Bosnia and Hercegovina

Academician, Stanko Bejatović, PhD, University of Kragujevac, Faculty of Law, Serbia

Goran Knežević, PhD, University of Belgrade, Faculty of Philosophy, Department of Psychology, Serbia

Božidar Banović, PhD, University of Belgrade, Faculty of Security Studies, Serbia

Đurađ Stakić, PhD, The Pennsylvania State University, Department of Psychology, United States

Milana Ljubičić, PhD, University of Belgrade, Faculty of Philosophy, Department of Sociology, Serbia

Zdravko Grujić, PhD, University in Priština in Kosovska Mitrovica, Faculty of Law, Serbia

Ivana Stevanović, PhD, Institute of Criminological and Sociological Research in Belgrade, Serbia

Zoran Pavlović, PhD, University of Business Academy Novi Sad, Serbia

Jelena Želeskov Đorić, PhD, American University of Cyprus, Department of Psychology, Cyprus

Milica Kolaković Bojović, PhD, Institute of Criminological and Sociological Research in Belgrade, Serbia

Valentina Ranaldi, PhD, Faculty of Law, Niccolò Cusano University, Rome, Italy

ORGANIZING COMMITTEE

Aleksandra Marković, PhD, Institute of Criminological and Sociological Research in Belgrade, Serbia

Nikola Vujičić, MA, Institute of Criminological and Sociological Research in Belgrade, Serbia

Milka Raković, Institute of Criminological and Sociological Research in Belgrade, Serbia

Aleksandar Stevanović, MA, Institute of Criminological and Sociological Research in Belgrade, Serbia

Andrej Kubiček, MA, Institute of Criminological and Sociological Research in Belgrade, Serbia

Nikola Drndarević, MA, Institute of Criminological and Sociological Research in Belgrade, Serbia

TABLE OF CONTENTS

Ivana Stevanović, Milica Kolaković-Bojović CHILDREN AND THE CHALLENGES OF THE DIGITAL ENVIRONMENT	9
Aleksandar Jugović CHILDREN IN THE DIGITAL ENVIRONMENT: BETWEEN WELL-BEING AND RISKS	27
Ivana Stepanović, Olivera Pavićević, Ljeposava Ilijić TRANSPARENT KIDS: HOW ALGORITHMIC SURVEILLANCE CHALLENGES THE PROTECTION OF CHILDREN'S RIGHTS ONLINE	39
Zoran Pavlović CHILDREN AND HATE SPEECH ON SOCIAL NETWORKS	51
Andrej Kubiček, Aleksandra Marković HATE SPEECH TOWARDS ROMA CHILDREN IN DIGITAL SPACE: DISCOURSE ANALYSES OF USERS' COMMENTS	65
Jelena Kostić, Valentina Ranaldi SOCIAL PEER VIOLENCE IN THE DIGITAL ENVIRONMENT - STUDENTS' ATTITUDES AND THE POSSIBILITY OF PREVENTION	83
Nebojša Macanović, Ružica Stojanović CYBERBULLYING AS A FORM OF PEER VIOLENCE IN SCHOOLS	97
Milena Milićević CYBERBULLYING AND CYBER VICTIMISATION: A LITERATURE REVIEW OF ASSESSMENT INSTRUMENTS	117
Katalin Csepregi, István Kovacs THE INCREASE IN DOMESTIC VIOLENCE DURING THE CORONAVIRUS PERIOD: WITH SPECIAL FOCUS ON CHILDREN POSITION	137

Hajdana Glomazić, Katarina Glomazić PARENTAL MEDIATION IN THE AGE OF DIGITAL TECHNOLOGIES: HOW TO PREVENT A CHILD BECOMING CYBERBULLYING VICTIM	153
Andela Đukanović COMBATING CHILD SEXUAL ABUSE ONLINE IN EUROPEAN UNION AND THE GENERAL PROCESSING OF ELECTRONIC COMMUNICATIONS	167
Aleksandar Stevanović CHILD PORNOGRAPHY ON THE INTERNET: CRIMINOLOGICAL ASPECT AND COMPARATIVE REGULATION	185
Jasna Hrnčić, Nina Lončar TECHNOLOGY-ASSISTED CHILD SEXUAL ABUSE, EXPLOITATION AND TRAFFICKING	199
Miodrag N. Simović, Azra Adžajlić- Dedović PROTECTION OF CHILDREN VICTIMS OF SEXUAL VIOLENCE AND SEXUAL HARASSMENT IN BOSNIA AND HERZEGOVINA	221
Nikola Vujičić, Nikola Drndarević OFFENDERS AND THEIR FAMILIES IN A DIGITAL ENVIRONMENT: A CASE STUDY OF PCI SREMSKA MITROVICA	239
ANNEXES:	
UN CONVENTION ON THE RIGHTS OF THE CHILD, GENERAL COMMENT NO. 25. (2021) ON CHILDREN'S RIGHTS IN RELATION TO THE DIGITAL ENVIRONMENT	255
UN KONVENCIJA O PRAVIMA DETETA: OPŠTI KOMENTAR BR. 25 (2021) O PRAVIMA DETETA U VEZI SA DIGITALNIM OKRUŽENJEM	277

CHILDREN AND THE CHALLENGES OF THE DIGITAL ENVIRONMENT

Ivana STEVANOVIĆ, PhD¹
Milica KOLAKOVIĆ-BOJOVIĆ, PhD²

Triggered by growing importance of digital environment, accompanied with significant opportunities and enormous challenges both- for children and those in charge of their wellbeing and personal development, authors have developed an idea of organizing the international scientific conference as a forum to discuss the most important issues, recent developments and perspectives, but also to prepare and issue the two thematic publications. Considering the recent developments of the international standards, especially a largely important UN CRC General comment No. 25 (2021) on children's rights in relation to the digital environment as the most important piece of the soft law legislation, the scope of this forum covers a wide spectrum of topics tackling children wellbeing in digital environment addressed by prominent members of academia, research community, psychologists, legal and social care professionals. The very purpose of this introductory paper is to shed a light on the theoretical, legal and practical discourse of this topic, but also to present the main attitudes of the authors who submitted their contributions to be presented and discussed during the conference.

KEY WORDS: children / digital environment / internet / online environment

¹ Senior Research Fellow, Institute of Criminological and Sociological Research, ivanacpd@gmail.com

² Senior Research Fellow, Institute of Criminological and Sociological Research, kolakius@gmail.com

1. INTRODUCTION

The rapid development of information and communication technologies, in conjunction with the “new reality” created in the context of the pandemic caused by the COVID 19 virus, has shifted a significant part of children’s activities into the digital environment, including both education and leisure. (Barnert, 2020, Minson, 2021) The dynamics of this process raised the question of the readiness of children themselves, their parents, teachers, professionals in the health, social protection and justice system, to address the challenges that this transition brings, including, but not limited to the following:

- Results and achievements in the learning process, health consequences due to lack of physical activity, including mental health- all related to the changed modalities of socialization.
- Risk of victimization, both in the context of hate speech, threats, blackmail and discrimination to which children are exposed in the online environment. This is of the great importance with regard to use of this environment to recruit children for sexual and other forms of exploitation, in both digital and conventional environment (Kolaković-Bojović, 2022).
- Finally, these changes have raised the question of the readiness of the police, the public prosecutor’s offices, courts and prison system to respond to the challenges of establishing mechanisms to facilitate reporting, more efficient investigation and prosecution of crimes committed in the digital environment.
- The focus must also be on the use of digital technologies as tools aimed at eliminating or reducing secondary victimization in proceedings in which children or minors appear as victims or witnesses. (Stevanović & Kolaković-Bojović, 2021)
- Last but not least, the capacities of modern technologies need to be further explored in the context of improving living conditions and treatment in penitentiaries, but also in the context of maintaining and improving the quality of family relationships, whether family separation is caused by deprivation freedom of parent and / or child.³

³ See: Kolaković-Bojović, Milica (2021) *Information and Communications Technology as a Tool to Substitute In-Person Visits in the Serbian Prison System During the Covid-19 Restrictive Measures*. Journal of Liberty and International Affairs, 7 (3). pp. 21-35. ISSN 1857-9760; Kolaković-Bojović, Milica, and Ana Batrićević. 2021. “Children in Correctional Institutions and the Right to Communicate with their Families during the Covid19 Pandemic.” Teme (4); Kolaković-Bojović, Milica and Batrićević, Ana (2020) *IMPACT ASSESSMENT OF Help e.V.’S RESOCIALIZATION PROGRAMME (Improvement of the treatment programmes in correctional institutions for adults and juveniles - SOE03-19)*. Institute of Criminological and Sociological Research, Belgrade.

2. UN CRC GENERAL COMMENT NO.25 (2021)

By adopting General Comment No. 25, On Children's Rights in Relation to The Digital Environment, in March 2021, the Committee on the Rights of the Child has taken a big step in understanding the new digital reality which largely affects the children, ranging from encouraging the development of their knowledge, skills and creativity, to generating numerous sources of danger and abuse. (Stevanović & Kolaković-Bojović, 2021)

In the context of the combating child victimization, the General Comment itself addresses several points of the great importance: Chapter VII recognizes the digital environment as a "playground" of for verbal, sexual and other forms of violence or for recruiting children for various forms of exploitation, while Chapter V (K) justice and legal remedies, paras 43-49) deals with the mechanisms of protection against abuse, ie reaction and support in a situation when abuse has already occurred. Finally, Chapter XII (B) deals with special protection measures in the context of the application of digital technologies in the protection of children from secondary victimization and as such is of great importance for the subject of this paper.

Chapter V (K), para. 43 recognizes the difficulties of detecting and investigating crimes in the digital environment, especially in the context of the need to require children to disclose sensitive or private online activities to the policy or prosecutor. It also recognizes the lack of reporting caused by the fear of peer retaliation or social exclusion. The commentary insists on establishing mechanisms for reporting this type of crime that are easily accessible and known to children and that ensure confidentiality. This provision should be interpreted in the context of the introduction of applications and digital tools that would provide children with free (legal) counseling and reporting of crime. The general comment insists that child counseling services must not be conditioned by prior notification or parental consent, as it is not uncommon for a child's fear of parental reaction to be the strongest barrier to reporting victimization. Such mechanisms could also be used to provide specialized support to child victims whose rights have been violated in or through the digital environment. (Stevanović & Kolaković-Bojović, 2021)

The Committee also recognizes the need for international and inter-ministerial cooperation and capacity building in the identification and protection of child victims in the digital environment. Such an approach would prevent re-victimization and secondary victimization of children in criminal proceedings, often caused by insufficient knowledge of information technology, digital environment and mechanisms. The Commentary also addresses the state's obligation to establish reparative mechanisms for child victims in the digital environment, including guaran-

tees of non-repetition (para. 46). Finally, General Comment No. 25 recognizes the need for child information and protection mechanisms in relation to the violation of their rights that need to be adapted not only to the child friendly language, but also in terms of accessibility modalities. In practice, this would mean that such information should be available in the form and in places like social networks, digital platforms, multimedia content, etc.), but also in other places in the real environment, so that they can be easily accessed by the child's parents or guardians. Also, accessibility of information for teacher and professionals who are in contact with children in the context of education, social and health care, as well as sports and other forms of organization of children's leisure time is of the vital importance, considering that they are often in a position to recognize that the child is a victim of violence.

Chapter XII (B) of the General Comment is devoted, among other things, to the digitization of court proceedings as a mechanism for protection against secondary victimization. Namely, the General Comment draws attention to the problem of using digital technologies in the context of surveillance systems, facial recognition software or risk assessment, which are used in the investigation and prosecution of criminal offenses, and in the context of potential violations of the child's privacy and dignity.⁴ The Committee recognizes that, where the digitalisation of court proceedings leads to a lack of personal contact with children, this may have a negative impact on rehabilitation measures and restorative justice based on developing relationships with the child. In such cases, and also when children are deprived of their liberty, States Parties should provide for personal contact in order to facilitate the content and cooperation of children with the judiciary and their smooth rehabilitation. (para. 120) This provision is in fact a kind of setting a "boundary stone" through which the digitalization of proceedings should not pass, ie recognizing the potentially negative aspects of the use of modern technologies in court proceedings.

3. EXPERT ATTITUDES

Recognizing the importance of an interdisciplinary approach to this topic, the Institute invited the most prominent experts in the field: members of academ-

⁴ More about the right to dignity see in: Kolaković-Bojović, M. and Grujić, Z. (2020) *Crime Victims and the Right to Human Dignity - Challenges and Attitudes in Serbia*. In: Yearbook. No. 3, Human rights protection : the right to human dignity. Provincial Protector of Citizens - Ombudsman ; Institute of Criminological and Sociological Research, Novi Sad ; Belgrade, pp. 239-269. ISBN 978-86-80756-36-3

ia, research community, psychologists, legal and social care professionals, to submit their contributions and to take part in the discussion. As a result of this process two publications have been prepared: Edited Conference volume *Children and challenges of digital environment* and the thematic section of the Journal of Criminology and Criminal Law, No. 2/2022.

In addition to this introductory paper, Edited Conference volume *Children and challenges of digital environment* includes 14 papers, but also English and Serbian full text version of the CRC General Comment No. 25.

Prof. Aleksandar Jugović⁵, PhD, in his paper *Children in the Digital Environment: between Well-being and Risks* presented in his paper is the analysis of the well-being and risks for children in the digital environment. The aim of this paper is to explain the thesis that information and communication technologies have a sociable and risky character for children. All children should have safe access to digital technologies and be empowered to participate, express their personalities, seek information and enjoy all the rights enshrined in the Convention on the Rights of the Child. The digital environment can negatively affect the lives of children, which raises the concern of parents and responsible adults for possible harmful consequences. Information and communication technologies create new forms of risks for children. These are the risks of contact, content, behaviour and health risks. The conclusion of the author is that state institutions have a primary obligation to respect, protect and realize the rights of every child to digital inclusion through the operation of relevant systems.

Ivana Stepanović, PhD⁶, Olivera Pavićević, PhD⁷ and Ljeptosava Ilijić, PhD⁸ in their paper *Transparent Kids: How Algorithmic Surveillance Challenges the Protection of Children's Rights Online* addressed the hidden danger of the algorithmic surveillance embedded in social media, recognizing that it is not simply an organizing principle that regulates visibility, sorts the content, and polices the online spaces. It is a business method of commodifying personal data that stimulates the production of various forms of digital violence due to its virality potential. Ethical guidelines that are set to prevent or penalise cybercrimes are always external to the logic of the market and the algorithms themselves because they prioritise engagement and reproduction of data at any cost. Children are especially vulner-

⁵ PhD Aleksandar Jugović is a Full Professor at University of Belgrade, Faculty of Special Education and Rehabilitation.

⁶ Ivana Stepanović, Institute of Criminological and Sociological Research, Belgrade and Institute of Advanced Studies Kőszeg.

⁷ Olivera Pavićević, Institute of Criminological and Sociological Research, Belgrade.

⁸ Ljeptosava Ilijić, Institute of Criminological and Sociological Research, Belgrade.

able because they are under constant surveillance while the price of opting out is too high. This paper analyses the processes of data commodification and stresses the importance of developing the legal framework for the protection of the digital rights of children while emphasising the need to reassess the impacts of surveillance practices and find comprehensive solutions against the systemic abuse of children's data online.

Prof. Zoran Pavlović, PhD⁹ in his paper *Children and Hate Speech on Social Networks* emphasizes that measures against discrimination at the international and national level, as well as the conditions for the use of social networks, cannot, however completely prevent the spread of hate speech. The debate on tightening sanctions against those who spread hate speech on social networks, and where children appear, should be led, but the right to freedom of speech and privacy, the standard of effective protection of children's rights and more should not be forgotten. Everyone is responsible, including social networks. The rights of the child are inviolable, as are the right to development or dignity. The ban on access to children's social networks is not a preventive measure, but a form of violence against them, additional victimization and not a positive educational mechanism. A responsible approach to the topic in the triangle of hate speech, children and social networks will not show its solutions through repressive measures of criminal law, but through prevention and creating zero tolerance for hate speech on social networks, regardless of whether it is posted by adults or children.

Andrej Kubiček¹⁰ and Aleksandra Marković, PhD¹¹ in their paper *Hate Speech towards the Roma Children in the Digital Space: Discourse Analyses of User's Comments* explore new modes of textual articulation of long-existing discourses towards a specific segment of a racialized ethnic minority, the Roma children. Considering the interactive dynamic nature of digital media portals, which allows users to interact with media producers, algorithms, and themselves by posting comments, authors seek new ways to explain this phenomenon, which further endangers the precarious social position of the youngest Roma. The article shows how the hidden aspects of minority children's lives are fantasized in the texts (re) generated by the readers, who became producers of media messages through digital technologies. Besides centuries-old stereotypes and interpretations of selective

⁹ Prof. Zoran Pavlović, PhD is a Full Professor at the Faculty of Law, University of Academy of Commerce, Novi Sad, Protector of citizens-Ombudsman of the Autonomous Province of Vojvodina, Senior Research Fellow

¹⁰ MA Andrej Kubiček is a Research Associate at the Institute of Criminological and Sociological Research, Belgrade.

¹¹ PhD Aleksandra Marković is a Research Associate at the Institute of Criminological and Sociological Research, Belgrade.

everyday experiences about Roma children, the article points out how irresponsible and unethical journalism can encourage the emergence of hate speech towards a specific group of children already in a disadvantaged social position.

Jelena Kostić, PhD¹² and Valentina Ranaldi, PhD¹³ in their paper *Social peer violence in the digital environment - students' attitudes and the possibility of prevention* analysing the phenomenon of the violence in communication between children and young people in the digital environment. As a result, their exposure to violence in the digital environment is increasing. This type of violence is specific, and the lack of direct contact can be encouraging for potential abusers. In addition, in some forms of digital violence, the reaction of the victimized person may be absent, and its absence may encourage further violence or even other forms of violence against him. During the pandemic caused by the COVID-19 virus, classes in schools were conducted online, and a measure of mandatory physical isolation was in force. This has certainly increased the use of social networks and messaging applications by children and young people. From April to June 2021 authors conducted two surveys through an anonymous survey among primary school students in the Republic of Serbia aged ten to fourteen. The aim of one research was to gain insight into students' attitudes and attitudes towards verbal peer violence in digital environments, and the other was to gain insight into students' attitudes and attitudes towards social peer violence in the same environment. Based on the results of the research, authors tried to give recommendations for the prevention of social peer violence in digital environments.

Nebojša Macanović, PhD¹⁴ and Ružica Stojanović¹⁵ in their paper *Cyberbullying as a Form of Peer Violence in Schools*, analysing the phenomenon of the violence by the means of the Internet, known worldwide as cyberbullying. They defined it as a general term for any communication activity using cyber technology that could be considered harmful to the individual or the common well-being. An increasing number of children and young people are being exposed to bullying via the Internet and additionally, the fact that it is still not recognized as a serious problem in society is worrying. One of the reasons why this trend is neglected lies in the fact that it occurs in the virtual world, and that it is not present in the "the real environment" of a child. The goal of this paper is to display empiri-

¹² Senior Research Fellow, Institute of Comparative Law, Belgrade, E-mail: j.kosti@iup.rs

¹³ Research Fellow in European Union Law, "Niccolo Cusano", University, Faculty of Law, Rome, Italy, E-mail: ranaldi@unicusano.it.

¹⁴ The University of Banja Luka, Faculty of Political Sciences, Study Programme in Social Work, Associate Professor

¹⁵ Daycare for children with special needs "Sunce Oberwallisa" Modriča, Master in Social Work

cal research that aims to determine the presence and the manner of cyberbullying among students in high schools in the municipality of Modriča, as well as the connection of this phenomenon with the educational and demographic characteristics of respondents. The research focuses on students and school as a place where these problems are often identified in young people. The results of the research indicate the existence of cyberbullying, but also reveal the causes and consequences of this phenomenon.

The issue of cyberbullying has also attracted Milena Milićević, PhD¹⁶ who prepared the paper *Cyberbullying and cyber victimisation: a literature review of assessment instruments*. She notices that the knowledge regarding cyberbullying and its consequences has increased during the past two decades, but also concludes that a more detailed insight into the characteristics of cyberbullying and cyber victimisation requires a significant diversity of measures. However, no agreement on the best measurement method has been reached. The present literature review aimed to identify and present the instruments and measures constructed and utilised to assess cyberbullying and/or cyber victimisation. A systematic search identified 2031 publications. The selection process resulted in 11 assessment instruments, which were analysed. According to the findings, the starting point in the construction or adaptation of assessment instruments specific to our context should be a consistent, enhanced and standardised definition of cyberbullying comparable to the ones used worldwide, followed by the precise criteria for the representativeness of the target population and carefully considered both socio-cultural factors and the time frame. Finally, author concludes that it is necessary to conduct comprehensive statistical analyzes in order to develop and verify the psychometric properties of the cyberbullying assessment tool that would be adequate for the assessment of this phenomenon in Serbia.

Katalin Csepregi¹⁷ and István Kovacs, PhD¹⁸, put the focus on *The Increase in Domestic Violence During the Coronavirus Period: With Special Focus on Children Position*. The focus of this paper is on protecting children from domestic violence. Domestic criminal law (Hungarian) has contributed to the criminalization of domestic violence, and it protects not only women but also children. The authors conducted a statistical analysis of data collected during the coronavirus period.

¹⁶ Senior Research Fellow, Institute of Criminological and Sociological Research, Belgrade

¹⁷ II. Master's Degree Student (MSc.), National University of Public Service, Faculty of Political Science and International Studies Master's Degree in International Public Service Relations

¹⁸ Ph.D. police major, assistant professor, University of Public Service Faculty of Law Enforcement Department of Law Enforcement Management Theory, and scientific secretary, University of Public Service Doctorat School of Law Enforcement

Statistical analysis includes a comparison of data on domestic violence during the coronavirus and two years before this period. The authors examine whether there was an increase in domestic violence, especially violence against children, during the coronavirus period. Restrictive measures (confinement or curfew) and psychological reactions have been identified as some of the leading causes that contribute to the increase in domestic violence.

How important role of the parents is in child cyberbullying victimization has been well recognized by Hajdana Glomazić, PhD¹⁹ and Katarina Glomazić²⁰ in their paper *How to Prevent a Child Becoming Cyberbullying Victim*. The issue of protecting children from Internet abuse cannot be viewed outside the importance of the parental role in that process. In this paper, authors investigate the relationship between parental mediation and child abuse through digital technologies. The aim of this paper is to examine whether parental mediation is a factor in reducing the risk of child abuse in the Internet space and whether intervention programs are designed to meet the needs of different categories of parents. The results have shown that parental mediation is a factor in preventing and reducing the risk of children online abuse. The extent of its success, among other factors, depends on the parental style and parental warmth. Furthermore, the data we have obtained suggest that it is necessary to deepen the current research on parental mediation in order to create better policies and program prevention.

In favor of the severity of a sexual abuse of children goes the fact that the most of the authors approached the conference topic from this perspective. Anđela Đukanović, PhD²¹ addresses the *Combating Child Sexual Abuse Online in European Union and The General Processing of Electronic Communications* starting from the position that the fight against child sexual abuse and exploitation is recognized as a priority for the EU, having in mind the significant increase in detected cases of online child sexual abuse in recent years. In order to resolve issue of online child sexual abuse, EU resorted to voluntary practice of processing online interpersonal communications by service providers, not based on firm legal basis. After extension of the scope of the Privacy and Electronic Communications *Directive 2002/58/EC*, this voluntary practice was paused, until the adoption of *Regulation (EU) 2021/1232* on a temporary derogation from certain provisions of *Directive 2002/58/EC*. Author concluded that, however, it seems that the imposed limitations on the right to private life and protection of personal data do not re-

¹⁹ Hajdana Glomazić is a research associate at the Institute for Criminological and Sociological Research of the University of Belgrade

²⁰ Katarina Glomazić is a Master of Psychology at King's College London, employed by NVIDIA, Reading, UK

²¹ Research Fellow, Institute of Criminological and Sociological Research

spect the essence of these rights, there was no detailed analysis of necessity and proportionality of general processing of content data and possible adverse effects on combating online child sexual abuse.

Aleksandar Stevanović²² approaches the topic of the sexual abuse of children from the perspective of the *Child Pornography on The Internet: Criminological Aspect and Comparative Regulation*. In order to contextualize the problem of child pornography, the author first strives to analyze the terms “pornography” and “child” in the context of the criminal law norm since it is imperative from a legal point of view to define what constitutes child pornography. Already at that step, many difficulties were pointed out, which are further implied on the adequate legal fight against child pornography. In the fight against child pornography. The influence of online technologies and Internet on the changed nature and phenomenology of child pornography was especially considered. Author especially pointed out that although the Internet makes it easier for criminals to engage in activities that fall under child pornography, child pornography would not have become so visible without the Internet. Although the constitution of incrimination of child pornography is deeply determined by the cultural and social basis in general, it is necessary to establish harmonization in terms of the legal fight against child pornography in order for it to be effective. In this context, we have analyzed several legal definitions of child pornography in both universal and regional legal acts.

Prof. Jasna Hrnčić, PhD²³ and Nina Lončar²⁴, identified e-tools and e-space as a fruitful ground for child abuse. In their paper, *Technology-assisted child sexual abuse, exploitation and trafficking*, they recognized a child sexual abuse (CSA) as one of the most devastating forms of human communication. In the last decades it is facilitated by information communication technologies (ICT). The authors analyse characteristics and specifics of ICT-assisted child sexual abuse, including exploitation and trafficking of children in order to provide better understanding of the phenomenon. Terms in the field have been examined, online environments as a risk factor analysed, prevalence of the phenomenon presented. Motivation, implicit theories and cognitive distortions of offenders are explained. Current typologies of ICT assisted CSA offences and offenders and risk factor for victimization are inspected. The differences and overlaps between terms and typologies in the field are discussed and barriers to effective prevention and intervention analysed. Urgency for effective social reaction to this blatant evil is emphasized.

²² Research Associate in the Institute for Criminological and Sociological Research in Belgrade, Serbia.

²³ Full Professor, Faculty of Political Science, Belgrade

²⁴ JU Dom starih “Pljevlja”, Montenegro

Academician Prof. Dr Miodrag N. Simović²⁵ and Prof. Dr Azra Adžajlić-Devović²⁶ presented the Bosnia and Herzegovina approach to the protection of child victims of sexual abuse. Their paper *Protection of Children Victims of Sexual Violence And Sexual Harassment In Bosnia And Herzegovina* recognizes the sexual violence as always a serious violation of the victim's personality, autonomy, psycho-physical integrity, self-control and self-esteem. Numerous other persons, thereby, including family members of victims, relatives, friends, acquaintances, etc., often appear as secondary victims. The prevalent victims of sexual violence in Bosnia and Herzegovina are female minors. Unlike sexual violence, sexual harassment is a delict of power aimed at "helpless victims" in non-democratic societies where there is no equality of rights for all citizens, but one part of society (men) seeks to maintain their positions of power by preserving the "patriarchal family" and sexual/gender discrimination and violence. The aim of this paper is to present the penal policy in the context of sexual violence against children in Bosnia and Herzegovina. In this regard, the protection of victims of sexual harassment and the results of the survey on fear of victimization - sexual violence and sexual harassment are analyzed. The results of the research should justify both the scientific and social significance of this paper.

Nikola Vujičić²⁷ and Nikola Drndarević²⁸ in their paper *Offenders and Their Families in A Digital Environment: A Case Study of PCI Sremska Mitrovica*, provided a review of the developments and characteristics of video visitation in PCI Sremska Mitrovica, with a focus on the contact between offenders and their families and children. The study draws upon data from fieldwork interviews with the prison employees and aims to understand experiences of using video visitation and their importance in the offender behavior as well as the prison system. The study gives voice to field experts with the knowledge and skills to suggest how video visitation impacts the offender behavior and its relevancy in the context of familial relationships. Moreover, it reflects on the nature of digital technologies in prisons and considers how they are embraced and managed in Serbia. Special focus is on the legislative framework in the Republic of Serbia.

In addition to the above presented papers, six papers submitted in Serbian have been published in the thematic section of the Journal of Criminology and Criminal Law, No. 2/2022.

²⁵ Vice-president of the Constitutional Court of Bosnia and Herzegovina, Full member of the Academy of Sciences and Arts of Bosnia and Herzegovina, Full professor at the Law Faculty, University of Bihać.

²⁶ Full professor in the Faculty of Criminalistics, Criminology and Security Studies at the University of Sarajevo

²⁷ Research Associate, Institute of Criminological and Sociological Research, Belgrade

²⁸ Research Assistant, Institute of Criminological and Sociological Research, Belgrade

Prof. Milan Škulić, PhD²⁹ in his paper *Criminal Law Reaction to Child Pornography/Juvenile Pornography – Realized/Created by Abuse of Computer Network/Communication by Other Technical Means* explained the basic characteristics of the criminal law reaction to child pornography, i.e. pornography of minors/juveniles, especially when it is realised using appropriate so-called high technology, which boils down to the misuse of a computer network or communication by other technical means. In the paper are presented the concept of pornography in the criminal law point of view, and author analyses the key normative characteristics of the criminal offense of showing, obtaining and possessing pornographic material and exploitation of a minor for pornography, (Article 185 of the Criminal Code of Serbia). The author also pays significant attention to comparative criminal law, explaining the basic characteristics of child pornography/juvenile pornography in German criminal law and in the criminal law of the United States.

Dragan Obradović³⁰ in his paper *Use of Audio-Visual Connection in Examination of Children in Criminal Proceedings - From the Judge's Angle*, explains that in numerous criminal proceedings, there is an increasing need in Serbia to examine children and juveniles as victims or as witnesses. Having in mind their age, their maturity, the examination of these categories of participants in criminal proceedings requires specially trained people - officials who will contact them from their first appearance either in the police, in the public prosecutor's office or in court. And for their additional protection in criminal proceedings, the legislator recognized the need to examine these vulnerable categories of participants in criminal proceedings can be done with the use of technical means - through audio-visual communication, which provides additional security for children and juveniles, so it is most important by legal regulations on criminal matters, he officially prescribed this possibility. During the 21st century, Serbia has technically equipped all higher courts with special rooms and audio-visual communication systems. In this paper, we pointed out the most important international and domestic regulations related to the protection of victims and are especially important for the protection of children in criminal proceedings, the way in which the use of audio-visual communication is regulated in the most important domestic criminal regulations. We also pointed out some cases from practice in which the examination of the injured - children and minors through audio-visual connection was applied.

The subject of the paper, *Audio – Video Link as An Instrument of Protection of a Vulnerable Witness and A Counterbalancing Factor* prepared by Ivana Miljuš, PhD³¹ is the dual function of audio - video link in criminal proceedings in which vul-

²⁹ Judge of the Constitutional Court of Serbia and the Full Professor at the Faculty of Law University of Belgrade

³⁰ Dragan Obradović, PhD, judge, Higher court Valjevo, Research Associate

³¹ Assistant Professor, University of Belgrade – Faculty of Law

nerable witnesses are examined - protection of witnesses and victims and ensuring the exercise of the defendant's right to examine witnesses. In the first part of the paper, the author analyzes the concept of "audio - video link", its legal nature, characteristics, roles and basic risks. The second part of the paper explores the normative and practical foundations of the protection of minors in criminal proceedings. The third part of the paper deals with the requirement to establish and maintain a balance of legitimate interests of enabling testimony and effective punishment, protection of the physical and mental integrity of witnesses and the right to defense. "In the balance test" of the European Court of Human Rights, the audio-video link is a "positive measure" of the state and a "counterbalancing factor". The subject of the paper is also the normative regulation of an especially vulnerable witness. The aim of this paper is to point out the importance of proper use of technical devices for transmitting images and sound during the examination of especially vulnerable witness, but also its potential risks, possible proposals to improve the normative basis for their application and basic principles of audio - video link in criminal procedure.

Ljubinko Mitrović, PhD³², Nikolina Grbić-Pavlović³³, Sonja Tomašević³⁴ in their paper *International Standards Regulating Protection Against Sexual Abuse and Exploitation of Children in The Digital Environment* presented the international legal framework, where there are a number of documents dealing with the protection of children, which are directly or indirectly related to sexual abuse and exploitation of children. Thus, in this paper, the authors will deal with international documents dealing with the protection against sexual abuse and exploitation of children with special emphasis on documents that directly deal with the protection of children from sexual abuse and exploitation in the digital environment. Due to the volume of international documents regulating the protection of children in this area, attention will be paid only to the most important international documents.

Vladimir M. Simović, PhD³⁵ and Marina M. Simović³⁶ in their paper *Child Pornography In The Light Of Computer Crimes: International Standards And Law Of Bosnia And Herzegovina*, addressed an international standards from a number of universal (UN) and regional (Council of Europe) documents, a large number of national legislations, including positive law of Bosnia and Herzegovina, that pro-

³² Ombudsmen BiH; Full professor, Law Faculty, APEIRON, Banja Luka

³³ Ministry of Interior, Republic of Srpska

³⁴ Senior Associate, Child Ombudsman Republic of Srpska

³⁵ Prosecutor in the BIH Prosecutors Office, Full Prof. Law Faculty University Vitez.

³⁶ Secretary in Child Ombudsman Republic of Srpska, Assoc. Prof. Law Faculty, APEIRON, Banja Luka

vide for several computer (computer, IT, information, cyber) crimes that violate or endanger various social values by using (or abusing) computers, computer systems or information technology. These are various forms of illegal activities of natural and legal persons, through, with the help of, through or by using computer systems, whether it is about old crimes take on new forms (forms of manifestation), or completely new crimes. Among these criminal offenses, computer crimes occur in a special, specific, or extremely dangerous way, especially for children and youth. This paper, in addition to the system of international standards and the basic characteristics of computer crimes, considers the content of computer crimes as mean of production or propagation of pornographic material in the legal system of Bosnia and Herzegovina.

Dragan Jovašević, PhD³⁷ recognizes in his paper *Encouraging Sexual Abuse of Minors Through Computer Devices* that sexual abuse of children and minors is an old crime that has been known since ancient times, both in the world and in our country. In modern criminal law, these sexual crimes acquire new forms of manifestation, especially if they are committed with the use of computer devices or systems. Thus, these criminal acts gain in importance due to the danger and severity of the consequences caused, ie a higher degree of guilt of their perpetrators. Legal protection of sexual freedom of minors from the abuse of computer information technology today occupies a prominent place in both international and national criminal law of the region. The paper analyzes the specific criminal offense of inciting minors to sexual exploitation through computer information technology in European documents, the law of Serbia and the law of the countries of the region.

In addition to the papers published in the Conference volume and the Journal of Criminology and Criminal Law, several prominent authors have submitted summaries/concept notes of their oral presentations.

Prof. Stanko Bejatović, PhD³⁸ in his presentation *Technology in a service of taking procedural actions in criminal proceedings where juveniles appear as victims or witnesses of crime* addresses capacities of the modern technologies, mostly ICT tools like video link, in elimination or reduction of the secondary victimization. The focus of his presentation is on the legislative framework of Serbia and perspectives to amend and improve it.

Sladana Jovanović³⁹ i Ljubinka Marković⁴⁰ in their presentation *Juvenile Offenders and Victims of Digital Violence* focus on the issue of digital violence

³⁷ Full Professor, Faculty of law, University of Niš

³⁸ Full Professor, Law Faculty, University of Kragujevac

³⁹ Full Professor, Law Faculty, University Union

⁴⁰ Psychologist at the Higher Court in Belgrade

among juveniles: factors, main characteristics, actual legal and social responses to it. The base for their presentation is the latest research results of judicial practice (of the Higher Court in Belgrade), data gathered by questionnaires filled out by juveniles from one high school in Belgrade, and other available studies on the topic. Some recommendations regarding improved response to digital violence among juveniles were made, having in mind General Comment No. 25 (2021) on children's rights in relation to digital environment adopted by Committee on the Rights of the Child.

Prof. Miodrag Simović, PhD⁴¹ and Prof. Mile Šikman, PhD⁴² in their presentation *The impact of the digital environment on children and responding to socially unacceptable behavior* analyze the increasing impact of the digital environment on the psychophysical development of children. The type and degree of impact can be different, and the consequence is always the same and is reflected in the harmful effects on psychophysical development children. At the same time, numerous studies on victims show that the real impact is high technology on the psychophysical development of children much higher than that expressed through the available data. The main reason for such a situation could be found in the reasons for not reporting this behavior by the victim or rather non-recognition of the harmful effects of high technology on psychophysical development of children. The authors also recognize the detrimental effects of secondary victimization, which they are very often covered victims of crime. In that sense, the question arises in which way society can most adequately respond to these behaviors. Different models of prevention can give promising results, but raise issues of protection of children's rights, including personal data. On the other hand, criminal repression, as the *ultima ratio*, has a full justification for its introduction, but also significant limitations. The authors pointed out that this is exactly the subject of their approach: prevention and suppression socially unacceptable behavior manifested by the use of high technology, either children are victims or actors of these behaviors.

Prof. Milana Ljubičić, PhD⁴³ and Prof. Đorđe Ignjatović, PhD⁴⁴ in their presentation *Victimization of young people on social networks - research results of Belgrade University students* presented results of their joint research the victimization of youngsters conducted among students of the University of Belgrade.

⁴¹ Vice-president of the Constitutional Court of Bosnia and Herzegovina, Full member of the Academy of Sciences and Arts of Bosnia and Hercegovina, Full professor at the Law Faculty, University of Bihać.

⁴² Associate Professor, Faculty of Security Studies University of Banja Luka

⁴³ Full Professor, University of Belgrade, Faculty of Philosophy

⁴⁴ Full Professor, University of Belgrade, Faculty of Law

In addition to the previously presented papers on the victimization, but also on the responsibility of juvenile offenders for crimes committed in digital environment, Mladen Jeličić, PhD⁴⁵ in his presentation *Misdemeanor responsibility of parents for child misdemeanor in the digital space* approaches to this issues differently- considering decreased age limits in terms of the active use of smart devices for activities in online space, he addresses it from the perspective of the parental responsibility for misdemeanor committed by their child under 14, who are therefore still irresponsible before the law.

4. CONCLUSIONS

Based on the main points addressed in the UN CRC General Comment No. 25 (2021), but also taking into account selection of topics made by the experts who presented their papers and the concept notes of their oral presentations, it could be concluded that victimization of children in digital space has been recognized as the one the main challenges of the digital environment. Both, CRC and international experts who took part in this initiative of the Institute of Criminological and Sociological Research agree upon the main issues attributed to this type of victimization:

- Lack of parental control mostly attributed to the insufficient digital skills of parents;
- Significant obstacles in investigation and proving this type of crimes;
- Harmful and longstanding influence of the cybervictimization on child personal development and wellbeing in general;
- Crucial importance of the prevention together with the strengthening capacities of professionals in contact with children as in police, prosecution service, courts, social protection and education sector as through the continuous raising awareness among children and their parents on how to deal with all challenges of digital environment and avoid child victimization.

In addition to this, some of authors well recognized that digital environment plays “two sides of one coin” role, so that digital environment as a space which daily hosts millions of children can be used as a fruitful environment to inform and strengthen them to report the crime.

The last, but not least, digital environment should be wider recognized and used to prevent secondary victimization of child victims and witnesses caused by direct contact with offender and the state officials within criminal procedure.

⁴⁵ Judge at the Misdemeanor Court Šabac, Research Fellow

REFERENCES

1. Barnert, E. 2020. "Covid-19 and Youth Impacted by Juvenile and Adult Criminal Justice Systems." *Pediatric Perspectives* 146 (2). DOI: <https://doi.org/10.1542/peds.2020-1299>
2. Kolaković-Bojović, Milica (2022) *Final report on the monitoring of court practice on the position of juvenile victims of crime before the courts in the Republic of Serbia in 2020*. Institute of Criminological and Sociological Research, Belgrade.
3. Kolaković-Bojović, M. (2021) *Information and Communications Technology as a Tool to Substitute In-Person Visits in the Serbian Prison System During the Covid-19 Restrictive Measures*. *Journal of Liberty and International Affairs*, 7 (3). pp. 21-35. ISSN 1857-9760
4. Stevanović, I. and Kolaković-Bojović, M. (2021) *Informacione tehnologije u službi zaštite deteta u krivičnom postupku*. In: Videolink i druga tehnička sredstva kao načini preduzimanja procesnih radnji u kaznenom postupku: (norma, praksa i poželjni slučajevi širenja mogućnosti primene). Misija OEBS-a u Srbiji, Beograd, pp. 61-77. ISBN 978-86-6383-112-4
5. Kolaković-Bojović, M. and A. Batrićević. 2021. "Children in Correctional Institutions and the Right to Communicate with their Families during the Covid19 Pandemic." *Teme* (4)
6. Kolaković-Bojović, Milica and Batrićević, Ana (2020) *IMPACT ASSESSMENT OF Help e.V.'S RESOCIALIZATION PROGRAMME (Improvement of the treatment programmes in correctional institutions for adults and juveniles - SOE03-19)*. Institute of Criminological and Sociological Research, Belgrade.
7. Kolaković-Bojović, M. and Grujić, Z. (2020) *Crime Victims and the Right to Human Dignity - Challenges and Attitudes in Serbia*. In: Yearbook. No. 3, Human rights protection : the right to human dignity. Provincial Protector of Citizens - Ombudsman ; Institute of Criminological and Sociological Research, Novi Sad ; Belgrade, pp. 239-269. ISBN 978-86-80756-36-3
8. Minson, Shona. (2021) "The impact of Covid-19 prison lockdowns on children." Oxford.
9. UN. 1989. "Convention on the Rights of the Child Adopted and opened for signature, ratification, and accession by General Assembly entry into force 2 September 1990, in accordance with Article 49."

10. Committee on the Rights of the Child General Comment No. 24 (2019), replacing General Comment No. 10 (2007) on children's rights in juvenile justice, Geneva, 18 September 2019.
11. Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment.

CHILDREN IN THE DIGITAL ENVIRONMENT: BETWEEN WELL-BEING AND RISKS

Aleksandar JUGOVIĆ, PhD¹

The subject of this paper is the analysis of the well-being and risks for children in the digital environment. The aim of this paper is to explain the thesis that information and communication technologies have a sociable and risky character for children. All children should have safe access to digital technologies and be empowered to participate, express their personalities, seek information and enjoy all the rights enshrined in the Convention on the Rights of the Child. The digital environment can negatively affect the lives of children, which raises the concern of parents and responsible adults for possible harmful consequences. Information and communication technologies create new forms of risks for children. These are the risks of contact, content, behaviour and health risks. The conclusion is that state institutions have a primary obligation to respect, protect and realize the rights of every child to digital inclusion through the operation of relevant systems.

KEY WORDS: children / digital environment / risks / well-being

1. INTRODUCTION

The digital environment consists of information and communication technologies (hereinafter: ICTs) that include the Internet, mobile devices, as well as digital networks, databases, content and services. It is estimated that over half of the world's population and 86% of Europe's population use the Internet, and that 1/3

¹ Full Professor, Faculty of Special Education and Rehabilitation, University of Belgrade, ajugovic1971@gmail.com

of the global population follows social media such as *Facebook*, *Instagram*, *YouTube*, *Tik-Tok* and others. About a third of all Internet users are children under the age of 18. In Serbia, over 70% of the population has access to the Internet and about 3 million are users of *Facebook* and *Instagram* (Jugović, 2021).

ICTs are changing the way people live in and the functioning of society. They are woven into our lives as intermediaries that transmit ideas, knowledge and information. ICTs do not affect children and adults *per se*, but they shape them according to their interests, values and interactions.

In the technological sense, “on stage” we have the integration of different media into one. What is a “smartphone” today? It is a technical means by which various media and the digital environment are “carried in your pocket”. In this way, it becomes a constant companion of man in real reality. ICTs are creating a new concept of time. It is the feeling that time passes faster. Also, it is harder to control time in activities within the digital environment than in the “off-line life” (Katzner, 2019).

In modern society, the classical distribution of social inequalities is changing through digital divisions that only reflects other forms of social differences (gender, geo-spatial, status). The distribution and dynamics of power in society are changing through the division into digital inclusion and exclusion, i.e. digital literacy and illiteracy (Hargittai and Walejko, 2008).

Children grow up in an age of “superconnected” and techno-social life through digital technologies that are the technical context of the digital environment. This environment was not originally designed for children, but today it plays a major role in their socialization and education (Chayko, 2019).

On the one hand, all children should have safe access to ICTs and to be empowered to participate, express their identity, seek information and enjoy all the rights enshrined in the Convention on the Rights of the Child. ICTs can be an important tool in the processes of education, socialization, freedom of expression, participation and inclusion of children. Thus, access to the Internet and digital literacy is part of the human rights of the child.

On the other hand, the digital environment can have a negative impact on children’s lives in various ways, which raises concerns among parents and responsible adults about the possible harmful consequences of the use of ICTs. Some previous research in the USA, from the beginning of the 21st century, when television was the dominant medium, indicated that children under the age of 18 saw about 16,000 simulated murders and about 200,000 violent acts on television (Jugović, 2014). Exposure to violence through modern ICTs is significantly higher than it was only through television content.

ICTs create new forms of risk for children. No child today is safe from the risks of the digital environment because they happen within the physical space of the house and the children's room. Physical space is no longer a barrier that protects a child from negative influences from the social environment. It has never been easier for a child to experience abuse or be exposed to violent and brutal content than it is today in the "digital age". The risks of the digital environment are especially related to vulnerable groups of children who already live with numerous adversities and deprivations (UNICEF, 2017).

The main goal of this paper is to explain the (hypo)thesis that ICTs have a potentially sociable and risky character for children. ICTs are both a "burden" and a "boon". They can both bring and take away a child's freedom, and be a means of both prosperity and alienation. There is a constant relationship between human nature and technology: ICTs can both improve and reverse human lives. We must face this fact as a society and with the constant aspiration to make the world and life a better place where the benefits of ICTs would prevail.

2. SOCIABILITY AND WELL-BEING OF DIGITAL TECHNOLOGIES FOR CHILDREN

Children are social beings who have a need for attachment and social belonging, and ICTs have social potential. Digital space is a place of socialization, research, self-actualization, defining the child's self and identity. This statement is best seen when we look at the most common activities of children in the digital environment. These are watching videos and photos, listening to music, recording and posting your own videos and photos on social networks, chatting, playing video games, watching feature films and series through digital services (Kuzmanović et. al, 2019).

For children who grow up with ICTs, "on and off worlds" are "mixed" as something that is "natural" for them. These are universes that permeate children. For children, digital life is real life and augmented reality. In the digital environment, children think, feel and act. Children experience pain, anxiety, joy, sadness and psychological presence when they use ICTs.

Generations growing up with ICTs are popularly called "digital natives" because the Internet and digital technologies are "close to the world". Today's children are entering the digital environment earlier and earlier. Some children have their first experiences with ICTs before the age of three. Today's 15-year-old child, in many settings, functionally uses ICTs as an adult over the age of 25 (Chayko, 2019).

The digital environment opens up opportunities for faster, more frequent and easier communication between children and their peers and parents. It has the potential to encourage the strengthening of friendships and for finding close people on online networks. Within the digital environment, a new language (like, share, selfie, subscript, screenshot, chat, *YouTube*, influencer) and new communication signs (emoticons, abbreviations and online slang) are being created.

This is where the “economy of attention” is born, where “like” has an emotional and social value that draws attention to the shared content of others. Living in a digital environment encourages the creation of “new politeness” in the form of ways of communication, such as following other profiles on social networks when they follow them or liking pictures of other children in response to their previous likes (Chayko, 2019).

Children in this world can interactively create digital content through games, social networks and communication with others. There are opinions that playing video games can contribute to the development of strategic thinking and logic in thinking.

In the digital environment, children can receive social support, quick access to important people, reduce feelings of loneliness and quickly find the necessary resources, information and people. Also, digital devices (telephone) are a means of controlling the safety of the child. Children can use these devices to call their parents when they are in trouble.

Through ICTs, children can coordinate daily activities, acquire knowledge, learn school materials, have fun, stand out from the stressful off-line environment, strengthen friendships, and gain status in the online community. Children develop a culture of participation through sharing and remixing content. The digital environment is also a space within which children can develop solidarity through group actions to help the vulnerable and reduce barriers to other cultures and nations. This environment enables the spread of a culture of free content, such as downloading music, images and lyrics (Chayko, 2019).

ICTs have the potential for children from marginalized communities to express their potential and break the cycle of inter-generational transmission of poverty and social exclusion. They also provide opportunities for learning and education for those children who are in remote and passive areas of the world, especially during wars, humanitarian crises and natural disasters (UNICEF, 2017).

ICTs are a part of the “culture of the children’s room” in which children are increasingly found in digital worlds, but also with less and less monitoring of their activities by parents. A special problem is that children enter the digital environ-

ment without developed and adequate digital skills, which exposes them to various risks. That is why it is important to recognize the risks to the rights and well-being of children that may arise in the digital environment.

3. DIGITAL LIFE OF CHILDREN AND FAMILIES

Digital media has become part of the children's family experience. ICTs change the dynamics of family life because they affect changes in communication within the family. Children observe and potentially adopt their parents' digital habits. Modern families use ICTs together and share content and events via emails and social networks. On the other hand, parents typically care about excessively used ICTs that interfere with learning and about the safety of children on social networks.

Research in the United States shows two basic patterns in the use of ICTs that depend on the material situation and educational level of family members. The richer and more educated strata strive for the ethics of empowering personal expression through educational content and personal development. The poorer and less educated strata prefer the ethics of polite connection where the priority is in contacts as the main purpose of using ICTs (Chayko, 2019).

This also raises the question of the role of family style of upbringing in mediation between children and ICTs. There are usually four ways in which parents mediate between children and the content they encounter in a digital environment. These are (Jugović, 2021):

- 1) *instructive*: parents actively participate in children's digital activities through discussion, explanations and evaluation of the content to which they were exposed;
- 2) *restrictive*: restrictions by which parents define the rules of how much (duration), when (at what time) and what (type of content) children can use from digital content;
- 3) *observational*: parents supervise, monitor and check what the child is doing online, with or without conversation with the child;
- 4) *without supervision*: parents do not monitor the child's use of ICTs or know minimally about what children do in the digital environment.

These models are not static, parents often change the way of mediation as the child grows or when they notice that the child has problems arising due to the use of ICTs. The choice of the model of this mediation can be related to the influence of the class, educational and social status of the family and the values of the parents.

4. CHILDREN'S RIGHTS IN THE DIGITAL ENVIRONMENT

The state, parents or guardians and institutions dealing with children have the primary responsibility to respect, protect and realize the rights of the child in the digital environment. First of all, children have the right to access the digital environment. Children have the right to privacy and family life in the digital environment, including the protection of personal data and respect for the confidentiality of their correspondence and private communication (UN Committee on the Rights of the Child, 2021).

They need to be protected from all forms of violence, exploitation and abuse in the digital environment. This should be done in a way that is in line with the best interests and developmental abilities of the child. Any protection measure against risks in the digital environment should not unnecessarily restrict the exercise of other rights of the child.

Children have the right to non-discrimination in the digital environment, especially vulnerable groups of children. They are the creators and distributors of information in the digital environment, which requires them to be digitally educated and to be given the right to freedom of expression and information. The digital environment provides special opportunities for children to exercise their right to participate in play and to gather and associate peacefully.

The child's right to education through the digital environment is especially important. Knowledge and resources from the digital environment should be available to all children in a way that is inclusive and that takes into account children's developmental capacities and the special circumstances of vulnerable children. Children need to develop their own digital, media and information literacy. Through digital civic education, children can acquire competencies that would allow them to engage safely and creatively in the digital environment (Committee of Ministers of the Council of Europe, 2019).

5. RISKS OF THE DIGITAL ENVIRONMENT FOR CHILDREN

Children are significantly more affected by the dangers of the digital environment than adults because they have less understanding of the risks they may be exposed to and suffer greater negative consequences. These consequences are in the spheres of risk to the well-being, enjoyment of human rights, healthy development

and overall well-being of the child. There are four related risk groups for children related to the digital environment. These are the risks of contact, content, behaviour and health risks.

5.1. Contact risks

A general risk for all Internet users, and therefore children, is the issue of monitoring, i.e. monitoring the digital habits of individuals by powerful owners of social networks and companies that sell their products. It is a universal issue of democracy, human rights and freedoms and the rights of the child in a situation where digital technologies are spreading to different areas of life.

The documentary *The Social Dilemma* (2020) by Jeff Orlowski, in which former creators of social network development, such as *Facebook* and *Instagram*, speak, convincingly shows how these networks exploit their own users for financial gain. The film points out that digital social networks have a strong negative effect on people's mental health because they encourage addiction, political manipulation and the spread of conspiracy theories. Internet companies are focusing their business on increasing and retaining users for as long as possible. It is in their interest, above all, to increase profits, where the problems of privacy and mental health of users become a "collateral damage". Every user of social networks must leave personal data that companies use for algorithms subsequently offering targeted content in advertising. Companies and advertisers on social networks "trade with the attention of users".

In addition to the stated risk of general manipulation and abuse due to the use of social networks, children may be at immediate risk of contact that would endanger their physical safety. These are situations of courting children in order to establish sexual contact, sexual exploitation and abuse, contact for the purpose of human trafficking and recruiting children on the Internet to commit crimes. Children can also experience contacts as a part of the activities of extreme political or religious organizations. This can also lead to situations of endangering the security of one's own computer data (spam, viruses, hacking, unsolicited emails), as well as endangering privacy due to the sharing of children's photos, both by children and parents.

5.2. Content risks

In the digital environment, children are exposed to various harmful contents that can have a potentially negative impact on the physical, emotional, cognitive

and social development of the child. Content risks exist in four domains: communication, violence, cultural models, and sexuality.

In the *field of communication*, the risks of content for children are discriminatory and gender stereotypical information, hate speech, false narratives, degrading and stereotypical portrayal of people and situations, manipulative speech of individuals, false news and misinformation, advocacy of unhealthy and dangerous behaviours (e.g. starvation and weight loss).

In the *field of violence*, children are exposed to risks from content that includes digital hate attacks, glorification of violence, incitement to suicidal behaviour and motivation to participate in violence criminal and terrorist activities.

In the *field of cultural models*, children encounter false scenes of other people's lives, so they can develop feelings of inferiority because others are "prettier", "more successful", "more liked" and "happier". The creation of a false digital elite and narcissistic culture is happening on social networks. There are numerous examples of culturally declining influences of certain "influencers" who express hatred, cruelty, vulgarity, arrogance and primitivism. Social networks are "full" of banalization of human relations and kitsch. Of course, this also exists outside the digital world, but it is easily accessible here and potentially harmful in the development of cultural habits and value systems.

In the *domain of sexuality*, these are pornography and pathological forms of satisfying the sexual needs of adults, such as paedophilia, sadism, masochism and exhibitionism. Children have easy access to all forms of sexual content all over the Internet, if there is no adequate control by adults. There are risks of early and excessive sexualization and the creation of false gender expectations in sexuality.

5.3. Behavioural risks

In the digital environment, due to the lack of physical contact and anonymity, the responsibility that exists in face-to-face communication is reduced, which encourages behavioural risks. Children can be both victims and perpetrators of risky behaviours. Characteristic forms of risk behaviours of children in the digital environment are:

- insults and digital stalking;
- virtual cruelty and harassment of others;
- disseminating sexualized images without the consent of another person;
- extortion of money and things;
- expression of hate speech;

- hacking and illegal downloading of content from the Internet and infringement of intellectual property;
- gambling;
- digital exclusion of other children from cyber groups;
- digital obedience under pressure from peers or seniors on networks;
- virtual voyeurism and exhibitionism (“selfie-mania”).

Behavioural risks also apply to digital behaviours that simulate real life and real intimacy with other people (Katzner, 2019). Excessive use of ICTs in children can create a new form of stress and fear due to the desire to maintain digital connectivity and respect on social networks. Today, many parents say that they have a problem with how to stimulate children outside the online environment because children express a state of “boredom” when they are not in the digital world and with a smartphone. Also, a significant parental problem is related to the organization of the child’s preparation for school, because the use of ICTs in children leads to a shortening of the period of learning and work on school obligations.

Finally, in the context of behavioural risk, the problem arises that children are under pressure to constantly check the messages and information they receive through digital devices. For modern children, the smartphone is continuously in their hands, as a kind of “mental and physical extension of the body”. Because of that, children have a problem with information overload and too many mental stimulation that they need to overcome. That is why there is a challenge for children and parents on how to pause and take a break from the use of ICTs and how to integrate “offline and online life” in the best way.

5.4. Health risks

Premature and excessive use of ICTs can create various health negative consequences for children. From the aspect of mental functions, these are challenges that arise due to long-term looking at the screen, such as problems with concentration, distraction, forgetting information and visual impairment. Digital content easily encourages the phenomenon of multitasking through fast and uncontrolled movement between different content and working on multiple content at the same time (Alzahabi and Becker, 2011).

In physical terms, the potential negative consequences are sleep deprivation, chronic fatigue, exposure to mobile device radiation, loss of willpower (“energy”), “sedentary” lifestyle and obesity. Health risks are reflected in the possible

development of dependence on Internet content and separation from the real world (Young, 1996). Digital activities with the highest dose of compulsiveness in children are: information retrieval, online games, chatting, pornography and gambling. Mood disorders in the form of anxiety and depression can also occur as a psychological consequence of all the above-mentioned health problems.

6. CONCLUSION

As human beings, we must strive to develop digital foresight. This paper shows that the digital environment is both a chance and a risk. An important lesson is that online and offline “worlds” need to be integrated into children’s lives. Man and technology do not have to be opposed. How we behave and what we strive for is our choice because we decide how to use technology. We need to be able to look at our own cyber life realistically and critically. In the digital environment, we must develop humanity and pass it on to children! We must strive to create a “virtual Kant” that should define the categorical imperatives of the digital age and the moral verticals of our digital present and future (Katzer, 2019).

Institutions responsible for the lives of children and parents have a key role to play in the search for these verticals. State institutions have a primary obligation to respect, protect and realize the rights of every child to digital inclusion through the operation of relevant systems, in particular education, child and social protection, media, businesses, civil society organizations, and children and their parents or legal guardians. The state should initiate and encourage the provision of a variety of high-quality content on the Internet that should have social and cultural benefits for children in support of children’s full development and participation in society. Children should be offered quality pro-social, educational, creative and entertaining digital content that is developmentally appropriate to the child’s needs.

Filtering risky content and blocking children, by itself, will not contribute to making the digital environment a safer and better place for children. Acquiring digital competencies of children through formal and non-formal education for safe, useful and creative use of ICTs is the basis of risk policies in the digital environment. Today, digital competencies are one of the most important prerequisites for the social inclusion of children in society. There are eight key digital competencies that children need to develop, according to the concept of digital intelligence (DQ)²: 1) digital identity; 2) digital rights; 3) digital literacy; 4) digital communication; 5) digital emotional intelligence; 6) digital security; 7) digital safety; and 8) digital use.

² According to DQ Institute: <https://www.dqinstitute.org/>

Finally, in the development of digital policies, children need to be asked how the digital environment affects their lives. Policies and initiatives should be based on scientifically established and up-to-date evidence of children's experiences in the digital environment.

REFERENCES

1. Alzahabi, R. & Becker, M. W. (2011) In defense of media multitasking: No increase in task-switch or dual-task costs, *Journal of Vision*, 11(11), pp. 102.
2. Chayko, M. (2019) *Superconnected: the Internet, Digital Media, and Techno-Social*. Beograd: Clio. [In Serbian].
3. *General Comment No. 25 on children's rights in relation to the digital environment* – the UN Committee on the Rights of the Child of 2nd March 2021. [In Serbian].
4. *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, June 2019. [In Serbian].
5. Hargittai, E. & Walejko, G. (2008) The participation divide: Content creation and sharing in digital age. *Information, Communication and Society*, 11(2), pp. 239-256.
6. Jugović, A. (2014) *Records in Anomie – Essays in the Science of Social Deviations*. Beograd: Institut za kriminološka i sociološka istraživanja. [In Serbian]
7. Jugović, A. (2021) *Children and Violence in the Digital Environment*. Beograd: Centar za prava deteta. [In Serbian]
8. Katzer, C. (2019) *Cyberpsychology. Online Life: How the Internet is Changing Us?* Beograd: Laguna. [In Serbian]
9. Kuzmanović, D. et al. (2019) *The Use of the Internet and Digital Technology by Children and Youth in Serbia*. Beograd: Institut za psihologiju Filozofskog fakulteta u Beogradu. [In Serbian].
10. UNICEF (2017) *Children in a Digital World*. New York: Division of Communication – United Nations.
11. Young, K. (1996) Internet Addiction: the Emergence of the New Clinical Disorder. *CyberPsychology and Behavior*, 1(3), pp. 237-244.

Prof. dr Aleksandar Jugović
Redovni profesor, Fakultet za specijalnu edukaciju i rehabilitaciju,
Univerzitet u Beogradu, Srbija

DECA U DIGITALNOM OKRUŽENJU: IZMEĐU BLAGOSTANJA I RIZIKA

Predmet ovog rada je analiza blagostanja i rizika za decu u digitalnom okruženju. Cilj ovog rada je objasniti tezu da informacione i komunikacione tehnologije imaju društveni i karakter rizika za decu. Sva deca treba da imaju siguran pristup digitalnim tehnologijama i da budu osnažena da učestvuju, izražavaju svoje ličnosti, traže informacije i uživaju sva prava sadržana u Konvenciji o pravima deteta. Digitalno okruženje može da negativno utiče na živote dece, što izaziva zabrinutost roditelja i odgovornih odraslih za moguće štetne posledice. Informacione i komunikacione tehnologije stvaraju nove oblike rizika za decu. To su rizici kontakta, sadržaja, ponašanja i zdravstveni rizici. Zaključak je da državne institucije imaju primarnu obavezu da poštuju, štite i ostvaruju prava svakog deteta na digitalnu inkluziju kroz rad relevantnih sistema.

KLJUČNE REČI: deca / digitalno okruženje / rizici / blagostanje

TRANSPARENT KIDS: HOW ALGORITHMIC SURVEILLANCE CHALLENGES THE PROTECTION OF CHILDREN'S RIGHTS ONLINE

Ivana STEPANOVIĆ, PhD¹

Olivera PAVIĆEVIĆ, PhD²

Ljeposava ILIJIĆ, PhD³

Algorithmic surveillance embedded in social media is not simply an organising principle that regulates visibility, sorts the content, and polices the online spaces. It is a business method of commodifying personal data that stimulates the production of various forms of digital violence due to its virality potential. Ethical guidelines that are set to prevent or penalise cybercrimes are always external to the logic of the market and the algorithms themselves because they prioritise engagement and reproduction of data at any cost. Children are especially vulnerable because they are under constant surveillance while the price of opting out is too high. This paper analyses the processes of data commodification and stresses the importance of developing the legal framework for the protection of the digital rights of children while emphasising the need to reassess the impacts of surveillance practices and find comprehensive solutions against the systemic abuse of children's data online.

KEY WORDS: algorithmic surveillance / social media / children's rights / digital rights, digital violence

¹ Research Fellow, Institute of Criminological and Sociological Research in Belgrade and Institute of Advanced Studies Kőszeg, ivana.stepanovic@iask.hu

² Research Fellow, Institute of Criminological and Sociological Research in Belgrade, oliverapavicevic4@gmail.com

³ Research Fellow, Institute of Criminological and Sociological Research in Belgrade, lelalela_bgd@yahoo.com

1. INTRODUCTION: DIGITAL RIGHTS OF A CHILD IN THE AGE OF ALGORITHMIC SOCIAL SORTING

The COVID-19 pandemic has exacerbated the digital transformation of the social, leaving children vulnerable to surveillance and data misuse without adequate legal protection against technologies they use every day for education, communication, and entertainment. Almost overnight, their everyday lives have shifted from physical spaces of schools and kindergartens to virtual classrooms and play areas. While all the efforts were focused on protecting the population from the imperceptible virus particles, little was done to safeguard children from the invisible dangers of the underregulated sphere of the internet. Sophisticated communication technologies expose children to intrusive algorithmic surveillance. Phones, tablets, cameras, smartwatches, and other gadgets can capture the most private data such as eye and muscle movements, breathing rhythms or tone of a voice that reveal the innermost thoughts, feelings, and intentions. Notorious for knowing people better than they know themselves, these technologies are the magnifying glass that makes children transparent, hackable, and manipulable. The digital transformation opened possibilities for distant learning and socialising along with remote surveillance and even algorithmically reproduced digital violence.

While there are many benefits of communication technologies, including the accessibility of information, availability of education and endless possibilities to connect with peers or play games online, there are also significant dangers that come with them. Misuse of data, cyberbullying and social media addiction are only some of the issues that are jeopardising children's rights and their wellbeing, while the impact of permanent algorithmic surveillance and social sorting remains to be a neglected issue. Many parents are not aware that everyday gadgets and devices with internet connectivity double as surveillance technologies or that the social media and gaming industry utilise the algorithms for the purposes of digital marketing and sales regardless of whether they are violating children's rights. These commercial practices of digital production can be interpreted as practices of exploitation of children through the extraction of their behavioural data. Given that normalised practices of data surveillance governed by platforms' algorithms routinely violate children's privacy and other rights and freedoms, it is questionable whether they truly operate in the best interest of the child.

Children are exposed and vulnerable online despite the efforts to create legislation to regulate their digital rights or build complex protective mechanisms such as parental controls and specialised platforms designed especially for children. The main challenge to protecting their rights in online spaces is the systemic data collection that is incorporated in both hardware and software and that draws the

economic processes on digital platforms from Google to TikTok. Just like grown-ups, children are involved in digital production and consumption. By participating in these processes, they become precarious producers, manipulated consumers and the products of their own labour. While the legislative framework for the protection of digital human rights in the age of algorithmic surveillance is still in its infancy worldwide, the basic principles of protecting children online are contained in international regulations such as the Convention on the Rights of the Child. Nevertheless, it is crucial to assess how fast-developing technologies collide with these principles and systemically violate children's rights.

2. ALGORITHMIC SURVEILLANCE AND SYSTEMIC EXPLOITATION OF CHILDREN ON DIGITAL PLATFORMS

One of the key issues with contemporary communication technologies is their capability to extract, store, analyse, interpret, and reproduce personal data. Monitoring users' behaviour while they are utilising the apps, platforms, mobile phones, and other technologies has been fully normalised even though these practices are in principle violating privacy rights. Algorithms built into these technologies are surveillance-based and created to serve the commercial needs of companies who create these technologies. Surveillance is therefore the method of digital production, while privacy is reduced from the right to protect personal data to the right to express consent for personal data collection and processing while retaining only partial control over the use of these data.

On the surface, digital technologies appear as useful tools for education, socialising, and entertainment. They were proven especially valuable during the COVID-19 pandemic when the whole world submerged in lockdowns and the internet offered a means to continue with normal life without leaving home. However, these technologies develop faster than it is possible to properly regulate them and prevent misuse and manipulation. It takes time for ethical conventions to adapt to new technologies, and it is especially difficult to regulate the imperceptible violations of human rights such as algorithmic surveillance that chronically lacks transparency and oversight. In the absence of legislation that would put algorithmic practices under scrutiny, privacy rights are systematically violated purely because the entire digital production relies on harvesting personal data. In other words, children's digital doubles are exposed to algorithmic surveillance in everything they do online, and this essentially means that they are being exploited. Their 'play labour' that consists of prosumption (Fuchs, 2014) of games, social media and other content is not considered illegal unpaid child labour, but the question is whether it should be.

Algorithmic surveillance and digital exploitation of children are potentially violating several articles of the Convention on the Rights of the Child. Namely, Article 14 stipulates that a child's freedom of thought and conscience should be respected, and it can be argued that social media algorithms could be violating this right. It is now commonly accepted that social media and other platforms use certain tools to manipulate opinions and impact the decision-making of consumers (Darmody & Zwick, 2020: 1). More broadly, the algorithms have become "the fundamental arbiters of human experience" even though they are "designed, programmed, and implemented by imperfect people who exist in a profit-first kind of world" (Johnson, 2021: 34-37). They determine what is going to be visible to whom according to their calculations and analyses of behavioural data. This means that they are infiltrating the social fabric by mediating our online searches as well as our digital production and consumption which allows the big tech companies to reproduce a parallel virtual world or a kind of a 'metaverse' that escapes the logic of ethics and law. The newly proposed Digital Services Act⁴ could be an attempt to regulate the online platforms and impose new rules to better protect users against the algorithms.

Children are not spared from the digital marketing machinery and algorithmic reproduction based on data surveillance. In fact, it can even be said that "the world in which the contemporary child is conceived and raised is one that is increasingly monitored, analysed and manipulated through technological processes" and that there is a substantial "power of algorithms within the everyday of the child" (Willson, 2018: 620). Even though the Article 17 stipulates that a child should have access to "information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health", it is questionable to what extent this diversity of information can be achieved given that the architecture of information on the internet is organised by the pre-set algorithms. But while there are various "types of algorithmic approaches in raising and imagining the 'ideal child'" (Willson, 2018: 620), there are also undercurrent tendencies to impose a certain market logic to the digital production and consumption or prosumption (Gerbaudo 2015: 81; Dyer-Witthford 2015: 92; Duffy et al 2021: 1).

These economic processes rely on big data surveillance that becomes overly intrusive and even "intimate" to such an extent that is capable of scanning thoughts and emotions to predict or even guide behaviour (Ruckenstein & Granroth, 2018: 1), which is why it routinely violates child's right to privacy defined in the Article 16 of the Convention. This article says that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence,

⁴ Digital Services Act eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN Accessed on 25.04.2022.

nor to unlawful attacks on his or her honour and reputation”. With normalised surveillance of communications technologies that have become a significant part of a child’s everyday life, it can be claimed that children’s digital privacy is consistently and systematically breached. Given that General Data Protection Regulation⁵ outlines the conditions under which it is legitimate to process personal data, online platforms are not engaging in unlawful practices, strictly speaking. Their business models involve the collection and analysis of data for profile targeting, and they offer the option for users to give their consent which is in line with the GDPR (Kardefelt-Winther, 2019: 22), but it is questionable whether such a mechanism satisfies the best interests of the child principle, especially if we consider the fact that very young children tend to use these platforms and consent to the processing of their personal data without knowing what it entails. Furthermore, it is possible to question the ethical justification of the intrusions into the privacy sphere even though they are not violating the existing laws, especially practices such as facial recognition and psychological profiling (Sharon, Koops, 2021: 331).

Algorithmic surveillance that is guided by the market needs of platforms inadvertently leads to exploitative practices of prosumption. Children are continuously engaged in unpaid digital labour of production and consumption on social media, gaming apps and other platforms. They are never simply passive users of technology, but rather active producers as their clicks, views, likes or gaming activities are the key production activities. At the same time, they are systematically monitored, analysed, and manipulated by the algorithms which consequently transform them into products of their own digital labour. As a result, children are involved in the circle of digital exploitation in which their personal data are the primary resource. These processes are rarely considered illegal even though in principle they violate article 19 of the Convention on the Rights of the Child⁶ which says that children should be protected from any form of exploitation and Article 32 that children should be protected from economic exploitation and from performing any work that is likely to be hazardous or to interfere with the child’s education, or to be harmful to the child’s health or physical, mental, spiritual, moral, or social development.

Algorithmic surveillance is already normalised and widely used even though its impacts on a child’s health, wellbeing, safety and security or freedom of thinking have not been thoroughly assessed. Due to the lack of high-quality research on these issues, there is a significant gap in knowledge on the effects of algorithms on children in general. On the one hand, the use of contemporary communication technologies significantly contributes to children’s well-being and development as

⁵ General Data Protection Regulation, (EU) 2016/679, gdpr.eu, accessed on 22.04.2022.

⁶ Convention on the Rights of the Child www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child, Article 19, accessed on 22.04.2022.

they use them for education and entertainment. However, there are also many adverse effects as children are exposed to cyber-hate, discrimination, and various types of cyber violence, including online sexual harassment, bullying, stalking and many others. These threats are palpable because they are associated with traditional crimes while algorithmic practices that are potentially manipulative and exploitative in elusive ways are rarely considered criminal offences. Current debates around “platform biometrics” (Crampton: 2019) and “behaviour profiling” (Eder, 2020: 23) are pointing towards a new understanding of digital criminology that includes normalised algorithmic practices that are not properly regulated by international or national laws. Imperceptible monitoring and profiling of children’s personal data is a potential threat to the collective rights and freedoms of children, and it requires further research, public scrutiny, and a more articulated legal framework that would ensure better protection of digital privacy, dignity, freedom of thinking and other rights of a child in the online world.

3. DIGITAL RIGHTS OF CHILDREN IN SERBIA

Serbia ratified the Convention on the Rights of a Child in 1990 and therefore accepted all obligations stipulated in this document⁷. It also has its own Personal Data Protection Law⁸ in line with GDPR⁹ aimed at safeguarding online privacy and Family Law that includes eight chapters dedicated to the rights of the child¹⁰. Additionally, the Serbian Government has a specialised department for cybercrime that defines types of offences that fall in this category, namely, child pornography, the spread of hate online and many others that directly or indirectly concern children¹¹.

Digital rights of a child in Serbia are mainly discussed in relation to classic cybercrimes and the security of children online and not in a broader context of digital criminology that is also concerned with algorithmic surveillance or manipulation and exploitation of children in less apparent ways. The main issue is children’s online security, and their protection against cyberbullying and various practices re-

⁷ Law on ratification of the United Nations Convention on the Rights of a Child, Official Gazette SFRJ – International contracts, No. 15/90 and Official Gazette SRJ – International contracts, No. 4/96 and 2/97

⁸ Data Protection Law, Official Gazette RS, No. 87/2018

⁹ General Data Protection Regulation (EU) 2016/679

¹⁰ Family Law, *Official Gazette RS*, No. 18/2005, 72/2011, 6/2015

¹¹ Government of Serbia, mup.gov.rs/wps/portal/sr/gradjani/saveti/Visokotehnoloski+kriminal (Accessed: 21.04.2022.)

lated to sexual abuse such as the so-called grooming, exposure to pornographic text and images, sexting and others (Pavlović, 2017: 124). The Information Security Law adopted in 2016 has been created with the aim to protect users against misuse of information and communication technologies, and Article 19a outlines the measures for the protection of children's safety and security on the internet¹².

However, existing research projects on the effects of information technologies on children in Serbia are scarce, and algorithmic practices are neglected. One of the valuable research projects is *Global Kids Online* conducted by the UNICEF Office of Research-Innocenti, The London School of Economics, and EU Kids Online in 2016¹³. One of the main conclusions of the research team is that Serbia does not yet carry out systematic research in the field despite the fact that information technologies play a central role in children's lives (Popadić et al. 2016: 5). According to this research, most of the children who participated in surveys use the internet every day, and every third child reported being exposed to aggression (ibid. 6). Moreover, the research shows evidence that children are regularly facing various risks while using the internet, and they include online bullying, exposure to upsetting or unwanted sexual content, meeting potentially dangerous online acquaintances in real life, password thefts, computer viruses and unauthorised use of personal data (ibid. 32). Additionally, the research findings show that the kids in Serbia are inclined to use pirate software more often than their peers in other European countries, which means that they are more vulnerable to computer viruses and malware and that they are at a greater risk of adopting a laid-back attitude towards piracy and perhaps breaking social norms in general (ibid. 41). While this research gives some insightful views of the dangers of using the internet, it also shows how children utilise electronic devices for educational purposes. Namely, it shows that use the internet to write, make presentations, source information, practice their skills and perform other activities, even though most of these practices are performed outside school (ibid. 25). These results are supporting the argument that children rely on information technologies to source information and empower themselves, which is why they have many digital skills (ibid. 29).

Among many benefits, information technologies offer better protection for children in court proceedings. It is especially important to emphasise the advantages of using video link in the court because this protects children and minors from secondary victimisation (Stevanović, Kolaković-Bojović, 2021: 61). It mirrors the principle of acting in the best interest of the child in the context of criminal proceedings, and Serbian institutions are currently working on developing a functional system of protecting children through adequate use of information technologies (ibid. 74).

¹² Information Security Law, Official Gazette RS No. 6/2016, 94/2017, 77/2019

¹³ Global Kids Online <http://globalkidsonline.net/> (Accessed: 22.04.2022.)

The main issue discussed Wider implications of information technologies and their impact on children's health, safety and wellbeing in Serbia and worldwide are not thoroughly researched. Effects of algorithmic surveillance and behavioural profiling are typically not discussed in the context of digital criminology even though they can be harmful and lead to breaches of fundamental rights guaranteed by the international treaties and Serbian laws.

4. CONCLUSION: TOWARDS SYSTEMIC SOLUTIONS FOR SAFER ONLINE LIVES OF CHILDREN

Understanding the intricate processes linked to the new digital economy is essential for investigating how information technologies work for and against children. Algorithmic social sorting should be the central concept in this analysis because it is the organising principle of online platforms and the basis of digital production. This new type of economy is sometimes referred to as "surveillance capitalism" (Zuboff, 2019) because it depends on the collection and processing of personal data. While children are playing with mobile phones, tablets, and personal computers, they are inadvertently and often without the knowledge of their parents being involved in production processes through which their behaviour online is being monitored, classified, interpreted and commodified. Algorithms extract their personal data to analyse their activities, decode their desires and predict their actions to monetise their play labour.

Even though these practices are normalised, they should be re-evaluated because of their potential to strip children of privacy and even freedom of thinking. Limiting the right to privacy to the triviality of consent and the partial control over the collection, sharing and processing of personal data results in weakening the concept of the private sphere and leaving children exposed and vulnerable. Platforms' algorithms are extracting children's data to create psychological profiles and target them with advertisements, offer them personalised content, decide what they will be able to see online and motivate them for certain actions. Since they are turning children's clicks, likes, comments and other activities into behavioural data that are further repurposed for their business objectives, the platforms are exploiting all their users for free labour and children are not an exception. In this sense, it is important to consider criminal aspects of business models that are based on algorithmic surveillance. The two new proposed EU laws, namely Artificial Intelligence Act¹⁴ and Digital Services Act¹⁵ have been introduced to address

¹⁴ Artificial Intelligence Act, artificialintelligenceact.eu/the-act/, accessed on 22.04.2022.

¹⁵ Digital Services Act, eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN, accessed on 22.04.2022.

some of these issues, broaden the scope of digital crimes and prevent or sanction some of the already established practices of algorithmic surveillance. However, it is also necessary to rethink the concept of child's privacy, especially in light of the intimate surveillance of children, their involvement in play labour of presumption and the possible impacts of algorithms on their health and wellbeing, access to information, freedom of thinking and exposure to violence.

REFERENCES

1. Artificial Intelligence Act, artificialintelligenceact.eu/the-act/, accessed on 22.04.2022
2. Convention on the Rights of the Child www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child, Article 19, accessed on 22.04.2022
3. Crampton, J. W. (2019) Platform Biometrics, *Surveillance & Society*, 17(1/2)
4. Data Protection Law, Official Gazette RS, No. 87/2018
5. Darmody, A., Zwick, D. (2020) Manipulate to Empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism, *Big Data & Society*, doi: 10.1177/2053951720904112
6. Digital Services Act, eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN, accessed on 22.04.2022.
7. Duffy, E. B., Pinch, A., Sannon, S., Sawey, M. (2021). The Nested Precarities of Creative Labour on Social Media, *Social Media + Society* 7(2) doi: 10.1177/20563051211021368.
8. Dyer-Witford, N. (2015). *Cyber - Proletariat: Global Labour in the Digital Wortex*. London: Pluto Press.
9. Eder, N. (2020) Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling in Ebers, M., Cantero Gamito, M. (eds) *Algorithmic Governance and Governance of Algorithms*, Data Science, Machine Intelligence, and Law, vol. 1, Cham: Springer, pp. 23-48, doi: 10.1007/987-3-030-50559-2_2
10. Family Law, *Official Gazette RS*, No. 18/2005, 72/2011, 6/2015
11. Fuchs, C. (2014). *Digital Labour and Karl Marx*. New York and Oxon: Routledge.
12. General Data Protection Regulation (EU) 2016/679, gdpr.eu, accessed on 22.04.2022.
13. Gerbaudo, P. (2012). *Tweets and the Streets: Social Media and Contemporary Activism*. London and New York: Pluto Press.

14. Global Kids Online <http://globalkidsonline.net/>, accessed on 22.04.2022.
15. Government of Serbia, mup.gov.rs/wps/portal/sr/gradjani/saveti/Visokotehnoloski+kriminal, accessed on 22.04.2022.
16. Information Security Law, *Official Gazette RS*, No. 6/2016, 94/2017, 77/2019
17. Johnson, J. D. (2021) Algorithm in Kennerly, M., Samuel Frederick, and Jonathan E. Abel (eds.) *Information*. New York: Columbia University Press, pp. 31-44
18. Kardefelt-Winther, D. (2019) *Child Rights and Online Gaming: Opportunities and Challenges for Children and the Industry*. Florence: UNICEF Office of Research - Innocenti
19. Law on ratification of the United Nations Convention on the Rights of a Child, *Official Gazette SFRJ – International contracts*, No. 15/90 and *Official Gazette SRJ – International contracts*, No. 4/96 and 2/97
20. Pavlović, Z. (2017) ICT (Information and communication technologies) based children's protection in Serbia, *Journal of Eastern European Criminal Law* 1, pp. 124-136,
21. Popadić, D., Pavlović, Z., Petrović, D., Kuzmanović, D. (2016) *Global Kids Online Serbia; Balancing Between Opportunities and Risks: Results from the Pilot Study*. Belgrade: University of Belgrade
22. Ruckenstein, M., Granroth, J. (2018) Algorithms, advertising and the intimacy of surveillance, *Journal of Cultural Economy*, doi: 10.1080/17530350.2019.1574866
23. Sharon, T., Koops, BJ. (2021) The ethics of inattention: revitalising civil inattention as a privacy-protecting mechanism in public spaces. *Ethics and Information Technology* 23, pp. 331–343 doi:10.1007/s10676-020-09575-7
24. Stevanović, I., Kolaković-Bojović, M. (2021) Informacione tehnologije u službi zaštite deteta u krivičnom postupku, in Beatović, S. (ed) *Videolink i druga tehnička sredstva kao načini preduzimanja procesnih radnji u kaznenom postupku (norma, praksa i poželjni slučajevi širenja mogućnosti primene*. Beograd: Misija OEBS-a u Srbiji
25. Willson M. (2019) Raising the ideal child? Algorithms, quantification and prediction. *Media, Culture & Society*, 41(5), pp. 620-636. doi:10.1177/0163443718798901
26. Zuboff, S. (2019) *The Age of Surveillance Capitalism*. London: Profile Books.

Dr Ivana Stepanović

Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

Dr Olivera Pavićević

Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

Dr Ljeposava Ilijić

Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

TRANSPARENTNA DECA: KAKO ALGORITAMSKI NADZOR UGROŽAVA ZAŠTITU PRAVA DETETA¹⁶

Algoritamski nadzor utkan u društvene mreže nije prosto sistem organizacije koji reguliše vidljivost, sortira sadržaj i reguliše prostore interneta već predstavlja mašineriju za trgovinu privatnim podacima. Ovaj ekonomski sistem motiviše proizvodnju različitih formi digitalnog nasilja i visokotehnološkog kriminala zahvaljujući njihovom viralnom potencijalu. Etičke smernice uspostavljene kako bi sprečavale ili kažnjavale krivična dela uvek su spoljašnja u odnosu na logiku tržišta pa i u odnosu na same algoritme jer prioritizuju angažovanje korisnika i reprodukciju podataka po svaku cenu. Deca su naročito ranjiva zato što su pod stalnim nadzorom dok koriste komunikacione tehnologije a cena odricanja od njih je previse visoka. Imajući u vidu kompleksne procese komodifikacije privatnih podataka, ovaj rad ukazuje na kršenja postojećih zakonskih regulativa i naglašava značaj daljeg razvoja zakonskog okvira za zaštitu digitalnih prava dece. Takođe, rad ističe važnost procene uticaja već normalizovanih praksi nadzora i pronalaženja sveobuhvatnih rešenja za zaštitu dece od sistemske zloupotrebe ličnih podataka i ugrožavanja njihovog blagostanja.

KLJUČNE REČI: algoritamski nadzor / društvene mreže / prava deteta / digitalna prava / digitalno nasilje

¹⁶ Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)

CHILDREN AND HATE SPEECH ON SOCIAL NETWORKS

Zoran PAVLOVIĆ, PhD¹

Measures against discrimination at the international and national level, as well as the conditions for the use of social networks, cannot, however completely prevent the spread of hate speech. The debate on tightening sanctions against those who spread hate speech on social networks, and where children appear, should be led, but the right to freedom of speech and privacy, the standard of effective protection of children's rights and more, should not be forgotten. Everyone is responsible, including social networks. The rights of the child are inviolable, as are the right to development or dignity. The ban on access to children's social networks is not a preventive measure, but a form of violence against them, additional victimization and not a positive educational mechanism. A responsible approach to the topic in the triangle of hate speech, children and social networks will not show its solutions through repressive measures of criminal law, but through prevention and creating zero tolerance for hate speech on social networks, regardless of whether it is posted by adults or children.

KEY WORDS: hate speech / social networks / strategy for the protection of children's rights / prevention / zero tolerance.

1. INTRODUCTION

Modern technological development accompanied by the development of the Internet takes on great importance in communicating, information and influenc-

¹ Full Professor, Faculty of Law for Commerce and Judiciary, University Business Academy in Novi Sad / Provincial Protector of Citizens, zoran.pav@hotmail.com

ing all of us, but also on the realization of the rights of all. Traditional media still have a role to play in all this, but there is a growing number of social networks and platforms that shows the growing presence of various forms of discrimination, and thus hate speech in communication, and often unforeseeable consequences of such expression. However, the reason for the availability of the Internet emphasizes the need to talk more about hate speech *online*, because it is different from *offline* hate speech. Spreading of hate speech through social networks and platforms does not have the time dimension as in the real world, where much more action must be taken to distribute it/expand it (hate speech), than writing graffiti, posters, printing books and similar.

Internet users have a special dimension of not being afraid of responsibility for the use of hate speech and its often inconceivable consequences. “False” anonymity of social networks and platforms, in the presence of another misconception that the usual rules of conduct and respect for the rights of others are not needed in *online speech* gives that dimension. This often results in content that shows the worst among people. The presence of children (of all ages) on social networks is the rule today, which then makes the consequences of “unarticulated” speech even more difficult, even more dangerous. Parts of the *online* identity can meet the *offline* world, so the consequences can spread indefinitely that way. Spreading hate speech through social networks, when the speaker is invisible to most users, makes such speech even more dangerous, but also the responsibility of those who maintain such media greater. Following the allegations of the United Nations Convention on the Rights of the Child, this is a speech that endangers the child’s right to life, survival and development.

All those, who spread hate speech, in this way cannot see the result of their words, but they also do not know what damage they inflict on the victims. Online communication includes written text as well as audio-video recordings, which means that it almost completely overlaps with the spread of *live hate speech* (face to face). Posting on a social network has the possibility of reaching a known or unknown number of users almost simultaneously, which results in a (spontaneous) reaction to such discriminatory communications, which can lead to *circulus inextricabilis*. From these characteristics of hate speech committed on social networks, we see that hate speech on the Internet has peculiarities and differences in relation to hate speech performed face to face. An additional feature of the phenomenon of hate speech on social networks is that there are special addresses where such behaviors are supported.

Hate speech is any oral or written statement of the will or thought of a person (speech) that is intended, directed, addressed to the public based on hatred or intolerance, regardless of how legal theory or individual legislation determines

them.² Hate speech committed through social networks, i.e. *online*, as well as hate speech committed face to face, i.e. *offline*, is subject to regulation by international treaties, national regulations and codes of conduct. The constitutionalisation of human rights, indirectly put the prohibition of hate speech on the level of a constitutional principle, which, along with the provisions of criminal law, regulations of electronic media, prohibition of discrimination, etc., makes the protection system almost complete. However, there are a large number of examples from media practice and on the available content of social networks that contain hate speech, where children are often found as subjects or objects.

Thus, hate speech (especially) towards children appears as a problem on a global level, because more developed technological solutions have more and more possibilities for spreading and inciting hatred and discrimination.

This type of speech is prohibited not only by constitutional acts, but also by numerous media or anti-discrimination laws which, based on relevant international standards, lay the groundwork for preventing the spread of hate speech towards all ages, where children are a particularly vulnerable category, and where an inadequate application of laws or not applying them at all, result in a criminal legal reaction.

That is why it is extremely important to approach this phenomenon differently than before, in order to protect the rights of the child, with increased attention and responsibility of all subjects, whether they are in the real or virtual world. In case of violation of (children's) rights on the Internet and through social networks, we now have two important tasks ahead of us: building a system of prevention and protection of children's rights on social networks and work on sensitizing all entities involved in repressive protection. For something like that, it is necessary to continuously work on the education of everyone who works with children, no matter if they are in education, police, judiciary or employees in other institutions of society. But let's go in order.

2. TWO EXAMPLES AND A FEW QUESTIONS

The attention of the professional and general public is occupied by cases in which children appear either as victims or as perpetrators. The specificity of the topic of hate speech on social networks only complicates this attention. The question is whether (without going into the technical aspects of this issue) to some in-

² Jovašević, D. (2022), Criminal responsibility and punishment for hate speech, Zbornik Govor Mržnje, PZGO - IKSI, p.109. The author talks about several people who may be affected by the consequences of hate speech.

dividuals access to social networks can be denied and if can on what basis, in cases of spreading hate speech, and not only if they are prominent politicians and issues related to electoral processes. Social networks when it comes to protecting children's rights, something that must be given special attention to. In such a case, we could include a case concerning specialized pages, which shows exactly how the protection system has its shortcomings, marked through the regulations on the protection of personal data, but not limited to them.

Namely, in the case of *CG v. Facebook* before the Court of Appeals in Northern Ireland³, the subject of the lawsuit was not hate speech, but a case of abuse of social networks and all the shortcomings of legal regulations. CG was sentenced in 2007 to unconditional imprisonment for committing several crimes against sexual freedoms. J. McCloskey, who was released from serving his prison sentence that year, wrote about this in 2013 on the specialized page "Let's protect children from predators2" on Facebook. His publication was related to articles in which CG, with a photograph, was described as the perpetrator of crimes against sexual freedoms. Other FB users immediately continued to supplement the page with data on CG, with the address where he lives or could live after his release from serving his prison sentence.

The proxies of CG demanded from FB that the disputed content on the specialized page be removed. And, after that was done, one of the family members of the victim published the previously downloaded content of the page "Let's protect children from predators2" on his personal FB account, emphasizing that CG is a danger to children. This page was also removed by Facebook. Defendant McCloskey was previously known in the *XY versus Facebook* case, because he had created a FB page "Let's keep children from predators", which was removed based on the decision of the High Court, so that he could immediately create a new page "Let's keep children from predators2". In this case, the Court of Appeals in Northern Ireland (2016) / NICA / stated that McCloskey endangered the privacy of CG, and that both McCloskey and Facebook are responsible for the misuse of personal data. In relation to FB, the High Court found that FB, as someone who maintains and manages the network, was obliged to follow the content of the specialized site "Let's keep children away from predators2", having in mind the fact that it was clear from the previous proceedings (*XY v. FB*) what McCloskey's activities are about on Facebook, and are responsible for the content of that page. FB appealed to the Court of Appeals, which found in the appeal proceedings that the fact of the earlier *XY* verdict could not be the basis for monitoring the activities of the "Keep children away from predators 2" page, because in that case Facebook would have

³ <https://globalfreedomofexpression.columbia.edu/cases/cg-v-facebook-ireland-ltd/> Decision of 19 January 2017

to monitor, contrary to the Directive. on e-commerce from 2002. The XY case was about harassment (which in the law of the Republic of Serbia would partially correspond to the criminal offense of Persecution), and not about the misuse of personal data. The court found that the misuse of personal data, as a result of which Facebook has not been fully informed of this possibility. However, in a letter from CG sent on November 23rd, 2013, Facebook was clearly and unequivocally informed about the abusive data of CG, and the page was removed on December 4th, 2013. The court therefore found Facebook responsible for the misuse of personal data only in a short period of less than a month at the end of 2013, because it did not remove the user's page in a timely manner after it was made clear. Finally, the Court found that Facebook Ireland is a "data controller" under the provisions of the UK Data Protection Act and is liable under the provisions of that regulation for the unlawful processing of personal data.

This case would open many questions related to the rights of the child and hate speech on social networks, although the court did not deal with that issue at all, starting from the lawsuit as it was formulated. But, after the case of *Spain versus Facebook*, the issue of the responsibility of the service provider on the social network and the content that is on it was finally defined. Many of the questions have still not been answered by the European Court of Justice at the European Union level, although it is indisputable that a service provider answers only if it intentionally endangers the rights of others. The responsibility set in this way does not exclude responsibility according to general legal principles, and especially in the light of the principle of the best interests of the child.

Another example, which has not yet fully received its epilogue, is in connection to social networks, but also to electronic and written media combined. In the Republic of Serbia, many preventive activities have been started in recent years to raise digital literacy, but this has not yet led to a reduction in hate speech and discrimination in which children appear as victims or perpetrators. Violence, including verbal violence (hate speech) that used to take place behind the school or in the yard of a house or building, is now increasingly happening on social networks.

Namely, at the beginning of December 2021, a 20-year-old girl KĐ passed away in Belgrade, whom newspaper articles and electronic media wrote that she had previously been a victim from her age of 16, of permanent discrimination and hate speech. Respecting the rule that cases that are ongoing, or that do not have their own court epilogue, are not commented on, we will, in principle, only present the data presented in public space. KĐ⁴ was a popular, young influencer who gathered hundreds of thousands of young people on various social channels, so

⁴ <https://www.euronews.rs/srbija/drustvo/28590/smrt-mlade-jutjuberke-kike-razotkri-la-stravican-svet-pretnji-i-vredanja-medu-mladima-na-internetu/vest>

she had more than 360,000 followers on Instagram. Among her audience, she became famous by playing Minecraft on YouTube and Twitch - a site for gamers. According to the media, the life violence suffered by the victim of KĐ was combined with violence on social networks, but no one read her calls for help, so the hate speech against KĐ was without an adequate social reaction. KĐ became additionally known when she got into a verbal conflict with BI, with whom she also discussed in the morning program of one of the TV networks with a national frequency, after which she stated in the daily Blic⁵ that she received various threats on the networks. “

But, with the death of KĐ, the hate speech on the occasion of that event did not end, because the rule was shown that one violence very often creates another violence. In this specific case, after the death of KĐ, BI, who was in a previous conflict with her, appeared as a new victim of hate speech. Some kind of persecution has started on social networks, with negative comments and discriminatory behavior towards BI; in which he was invoked responsible for the death of KĐ. ⁶That is how it came about, that hate speech continued on social networks, which consequently led to the death of KĐ.

Some children are obviously more exposed to public court and hate speech, and go through digital violence or cyber bullying. Given that, we often do not have feedback from children on the types of violence to which they are exposed, this raises the question of the responsibility of service providers - social networks. In a real or offline environment, hate speech is still easier to identify and it can be reacted to it faster. That is why the issues of violence in the virtual world, including hate speech, must be legally resolved in any public space, including social networks.

This especially calls for social reaction and the creation of a protection system, because according to UNICEF Global kids online research conducted in Serbia, 94% of primary school students and 99% of high school students have a mobile phone, 89% of primary school students and 92% of high school students have access to the Internet and 84% of high school students exposed themselves to some of the risks on the Internet. According to that research, as many as 37% of elementary school students and 66% of high school students were exposed to violence on social networks, i.e. hate speech, while about a third of them heard that their friends suffered the consequences of discrimination on social networks.⁷

⁵ <https://www.blic.rs/slobodno-vreme/vesti/ubila-se-srpska-lepotica-a-njen-poslednji-stori-je-najtuznija-prica/18jj40k>

⁶ <https://www.alo.rs/zabava/estrada/574820/baka-prase-kristina-kika-djukic-bulging-sajber-nasilje-jutjuberka-izvesila-samoubistvo/vest>

⁷ Popadić, D., Pavlović, Z., Petrović, D. and Kuzmanović, D. (2016) *Global kids online Serbia: Balancing between Opportunities and Risks. Results from the Pilot Study*, Belgrade: University of Belgrade, at: www.globalkidsonline.org/serbia

The rhetorical question we will ask here is, what kind of legislative framework is needed, which would be hate speech with the consequences shown in these two examples and children at risk of hate speech on social networks, in order to complete the social reaction in the system of protection against hate speech in general, and especially towards children.

3. LEGAL REGULATIONS ON HATE SPEECH IN THE REPUBLIC OF SERBIA

In the Republic of Serbia, the constitutional text nowhere directly mentions hate speech, but through the constitutionalised right to freedom of speech, which has its positive limitations, we can conclude that the constitutional framework has been established. The constitution, in its article 21, defines according to the principle of prohibiting discrimination, that any kind of discrimination, direct or indirect, or on any ground, in particular, race, sex, nationality, social origin, birth, religion, political or other opinion, property, culture, language, age and mental or physical disability is prohibited. Within the framework of “Human Rights and Freedoms”, it was proclaimed: “Prohibition of inciting racial, national and religious hatred”. Any incitement and incitement to racial, national, religious or other inequality, hatred and intolerance is prohibited and punishable.

Along with the strategic documents, we can say that there are several specific legal mechanisms for protection against hate speech, which are based on two legal frameworks: the Law on Protection against Discrimination and the Law on Information and Media.

If it is a matter of protection of the rights of the child on the basis of Article 16, paragraph 2 of the Constitution of the RS, we can also apply the Law on Ratification of the UN Convention on the Rights of the Child.

If hate speech incites violence and hatred, the Criminal Code applies. However, the relatively modest jurisprudence in the field of hate speech (especially on social networks) also points to the fact that it is still necessary to work on creating a protection system in this area and that many available mechanisms are not effective, proportionate and dissuasive. In future amendments to the relevant regulations, a strict distinction should be made between hate speech and harassment and degrading treatment, which overlap in practice. Also, prosecutors very often do not recognize hate speech and do not act on criminal charges. In any case, at the level of statistical error, there are cases in which public prosecutor’s offices acted on their own initiative, if they heard about the consequences of hate speech on social networks.

Judicial practice is also very problematic, as judges in some cases have not recognized hate speech, and often recognize freedom of expression as an inviolable value. The right to freedom of expression is an element of any democracy and is protected even if information can be shocking and disturbing, it must be limited when a speech is considered hate speech. This is of particular importance in multicultural societies, which are in transition, with a difficult past and which have an underdeveloped level of human rights culture and media literacy. That is why we must work, similar to zero tolerance for violence, and the rule of zero tolerance for hate speech. This justification makes sense if it is a speech in which both the subject and the object of hate speech are adults, but the situation can be viewed differently if children appear as victims of hate speech, when the consequences are more frequent and severe, so society's reaction is mandatory. .

Hate speech itself was introduced for the first time in our legislation in the Law on Prohibition of Discrimination, which prohibits hate speech, and can be called an example of good practice and providing legal protection to particularly vulnerable groups and individuals in society, although it does not specifically mention children, except in a broader interpretation.

The advanced solutions from this law (Article 11) are commendable, due to the definition of hate speech, but we must emphasize that it is not fully in line with the definition from the ECRI Recommendation no. 15, and second, does not differentiate between harassment and degrading treatment. Hate speech defined as *the expression of ideas, information and opinions that incite discrimination, hatred or violence against a person or group of persons because of their personal characteristics, in public media and other publications , at gatherings and places accessible to the public, writing and displaying messages or symbols and in another way, for the purpose of acting towards third parties, and is encouraged by expressing ideas and opinions that lead to discrimination, hatred or violence .*

The very definition of hate speech lacked social networks, which was certainly not noticeable at the time of writing, and the examples given, as well as other real-life examples, show the need to either set a more general definition or introduce social networks as places of execution.

Incriminations of certain behaviors in the Criminal Code, ⁸directly or indirectly hate speech, include criminal offenses against freedoms and rights of man and citizen, criminal offenses against parts and reputations, criminal offenses against the constitutional order and security of the Republic of Serbia, criminal

⁸ Criminal Code of the Republic of Serbia “Official Gazette of the RS”, No. 85/2005, 88/2005 (correction), 107/2005 (correction), 72/2009, 111/2009, 121/2012, 104/2013, 108 / 2014, 94/2016, 35/2019)

offenses against public order and peace, criminal offenses against humanity and other goods protected by international law.

This does not end the catalog of criminal acts in which criminal acts with elements of hate speech are found, but these are the ones in which it most often appears as a possible act of execution. We must draw attention to the fact that these are not criminal acts - hate crimes, but criminal acts resulting from hate speech. The difference is discrete, but it exists. Namely, the phenomenology of hate speech requires us to have mechanisms that enable an adequate social reaction to hate speech, especially when it is done through social networks. Prosecuting social networks, as well as individuals for hate speech, is therefore not an easy task, and implies appropriate changes in legislation, but also a change in the attitudes of prosecutors and courts in the prosecution and trial of such crimes. Only as an example, will we single out the acts of execution from Article 387 (racial discrimination) of the Criminal Code. Disseminating and making publicly available texts, images or any other representation of ideas or theories advocating or inciting hatred, discrimination or violence against any person or group of persons based on race, colour, religion, nationality, ethnic origin or to some other personal trait (which extends the notion of victim to other forms beyond racial discrimination).

Penal provisions on hate speech are contained in regulations other than the Criminal Code, the Law on Prohibition of Discrimination and the Law on Public Information and Media, as well as in other media laws that contain penal provisions.

Regardless of the legal framework for sanctioning hate speech, there is still no unified data on which crimes would be dealt with and which courts will be tried at, but a number of cases can be identified through reports on the work of independent institutions. However, the relatively small number of processed reports or verdicts shows not just that there was no hate speech, but that the authorized persons still have not shown a sufficient level of sensitivity for this act of execution, and then they also have not done anything in connection to these life events.⁹

4. CONCLUDING CONSIDERATIONS

We will repeat that the rights of the child are inviolable, as well as the right to develop or to dignity. These rights need to be appreciated in each specific case, al-

⁹ Pavlović, Z. (2022), Hate speech, violence and disseminating of false news on the global social networking highway, p. 159, Hate speech, Proceedings, PZGO - IKSI, Belgrade

ways keeping in mind the best public, and above all the best interests of the child.¹⁰ We can freely state that these rights are threatened especially on social networks, through hate speech. Therefore, in the part of the academic community, the child's rights issues have been conducted in the last two decades, in the last two decades of social responses to hate speech, especially children and hate speech on social networks. Pluralism of attempts to systemically approach this topic, due to its specificity, but both of constant and quick changes and modalities of hate speech, has not yet led to a satisfactory result. The consequences of hate speech can be large and worrying, not violating the rights of those who are on social networks, but also those not their users. Special reason for processing the topic of children and speech hate on social networks is the fact that domestic violence does not report or apply very rarely, and that hate speech is not experiencing in this type of violence (Competent) Subjects in general as violence and crime.

Most children do not report violence because they are afraid that they will be confiscated a computer or mobile phone, which is a special form of violence against children today, not a way of solving problems. Children are ashamed to say what is happening to them and do not want to confide to their parents or someone older, which is to be expected if we take into account that we are talking about children or young people.

As it is about children and a younger population, which suffers violence often from their peers, but also from adults, beside constant education and encouragement to report the incident, victims need to be pointed at the fact that, although violence occurs in a virtual rather than real space, it, the violence, should not be ignored and be silent about it. Threats of violence (whose overture are insulting and discriminatory messages) are the use of hate speech or potential violence in real life that the victim is put into appearance. The children victims should be encouraged to talk about violence experiencing, to report threats and, in accordance with particular violence, seek appropriate legal protection.¹¹

This protection can be realized in different ways, through the strengthening of the existing legal framework, raising responsibility of the service provider on social networks, digital literacy and building and strengthening the awareness of the affirmative role of speech, not in its altruistic sense, but in a counter - narrative relations to hate speech.

Given that the area of protection of the child's rights, in the digital age, is a topic that is still at the beginning, and not in precise frameworks or protection mech-

¹⁰ Pavlović, Z. (2018) Protection of Privacy and dignity of a child in media space, Zbornik Pravda po meri deteta, IKSI, Beograd, p. 91.

¹¹ Vilić, V. (2022) Vršnjačko nasilje kroz govor mržnje na društvenim mrežama, p.169, Zbornik Govor mržnje, PZGO IKSI, Beograd

anisms, the problem of speech of hate on social networks is the problem of society and affect children and young people. The development of modern technology and general internet availability made that hate speech becomes an exceptional problem at the international level. Based on its characteristics, social networks have become a big problem in efforts that hate speech is to be suppressed. The absolute control of putting on social networks does not exist as well as the possibility of absolute monitoring of the entire content that is available in virtual space, which makes the possibilities of promoting hatred, hostility, discrimination or intolerance increased.

Therefore, social networks call users to report inadequate content, for further reaction.

In hate speech, one of the most important tasks of theory and practice is delimitation to the basic human law - freedom of expression. If we have in mind that children and young people are especially vulnerable and sensitive even having in mind that they are the largest beneficiaries of social networks, this task looks very responsible. As an example of good practice, and watching things *de lege ferenda*, maybe the practice of some other countries should be also considered.

It starts from the point of view that a speech that can cause detriment to individual rights and lead to violence, discrimination or hostility, freedom of expression or freedom of speech can still be limited. In the Federal Republic of Germany, they have a very strict approach to sanctioning hate speech from the mid-20th century. Laws on preventing hate speech were created as a result of the experience of this country with Nazism and Holocaust. Today's Social Network Law (Netzwerkdurchsetzungsgesetz - Netzdg), was adopted in 2017 with the aim of preventing online hate speech and the spread of fake/false news. This law obliges social media platforms with more than 2 million users to remove content that is "obviously illegal" within 24 hours after notification done by users, i.e. to examine legality and remove suspicious content within 7 days. The law prescribes penalties for social networks in the amount of up to 50 million Euros. Such commitment and high punishments have influenced Germany at an extremely small rate of hate speech on social networks in general. Perhaps this way of regulating is a good example of harmonization of national and communitarian law, and modern tendencies.

Children and young people, although skilled in the use of new technologies, fact is that they do not have enough life experience or critical awareness to see all online and offline hazards. That is why modern education on digital culture is the basis of fighting hate speech on digital networks, with good regulations.

Traditional legislation in the Republic of Serbia written at a time when internet and social networks have not yet had this role in public and private life requires

adapting to new circumstances today. What does not necessarily involve the definition of hate speech in various legal documents of domestic and international rank, but also consideration of repressive nature, bearing in mind the fact that as a victim of hate speech on social networks is most commonly appears a child.

The phenomenology of the consequence of the speech of hate on social networks is correlated with the possibilities that social networks provide. So, if there is a criminal response to the consequences of hate speech, the issue of responsibility should not be concerned about only an individual executor, but also the platform provider. But to react to criminal law in such a situation, it is necessary to harmonize regulations that regulate the responsibility and level of social network responsibility in general. Because, what is a characteristic of criminal law is that without precise definition of social networking obligations for removing the content of hate speech, there can be no criminal responsibilities.

The users of social networks are expected to refrain from communicating hate speech, and social networks are responsible for the publication of the user's illegal content. The experience caused by the fight against some other phenomena, such as the fight against discrimination, indicates that the successful social reaction to hate speech and its consequences is only possible by creating protection systems in the world of multiple competencies, technological achievements and technical solutions, created using social networks.

It is undeniable the importance of social networks in the realization of the right to freedom of expression, but also the protection of the rights of individuals. In order to achieve preventively better results, it is necessary to unify the existing definition of hate speech and international standards and the Ekro number 15 recommendations, which would result in distinctness between hate speech and harassment and degrading treatment.

In mandatory training programs, not only students of the Faculty of Law or Judicial Academy should be included but also acting judges and prosecutors – also should introduce education of those who work on hate speech, with special reference to social networks. In other words, in addition to drafting a national strategy for combating hate speech on the Internet and social networks, it is necessary to work on harmonizing legal texts based on such a strategy, which should use the experience gained by independent bodies in RS. Social reaction through the norms of criminal law would be and is only the last measure in preserving the rights of the child on social networks.

Citizens, and especially children who use both internet and social networks, have the right to enjoy full legal protection available, while being *online* as well as *offline*, which is also in line with the Council of Human Rights Council No. 20 / 08 in 2012, therefore protected from hate speech, violence and false news.

Responsible access to the topic of the child's rights and hate speech will be thus achieved mostly through the prevention and creation of zero tolerance regarding hate speech on social networks, regardless of whether growing adults or children are placing it on, and only after this, with the criminal law measures also.

REFERENCES

1. JOVAŠEVIĆ, D. (2022), Criminal Responsibility and Punishment for Hate Speech, Zbornik hate speech, Pzgo - Iksi,
2. Popadić, D., Pavlović, Z., Petrović, D. and Kuzmanović, D. (2016) Global Kids Online Serbia: Balancing Between Opportunities and RISKS. Results from the Pilot Study, Belgrade: University of Belgrade, at: [www.globalkidsonline / Serbia](http://www.globalkidsonline/Serbia)
3. Pavlović, Z. (2022), Hate Speech, Violence and Dissemination of False News on the Global Social Networking Highway, Hate speech, Zbornik, Pzgo - Iksi, Belgrade
4. Pavlović, Z. (2018) Protection of Privacy and Dignity of a Child in Media Space, Zbornik Pravda Po Mere Kijeta, Iksi, Beograd
5. Vilić, V. (2022) Peer violence through hate speech on social networks, P.169, collection hate speech, PZGO Iksi, Belgrade
6. [HTTPS://globalfreedomofexpression.columbia.edu/cases/cg-v-facebook-ireland-ltd/](https://globalfreedomofexpression.columbia.edu/cases/cg-v-facebook-ireland-ltd/) Decision of 19 January 2017.
7. <https://www.euronews.rs/srbija/Drustustvo/28590/smrt-mlade-jutjuberke-kike-razotkrila-stravacan-svetvetnji-i-vrevi-metu-mladima-na-internetu/vest>
8. <https://www.blic.rs/lsobodno-tra/vesti/ubila-se-srpska-lepetica-a-nim-jemstiri-stori-je-nuzni-prica/18jj40k>
9. <https://www.alo.rs/zabava/estrada/574820/Baka-prase-kristina-kika-djukic-buling-sajber-nasilje-jutjuberka-izvesila-samoubisto/vest>
10. Crime Code of the Republic of Serbia ("Official Gazette of RS", No. 85/2005, 88/2005 (correction), 107/2005 (Correction), 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019)

Prof. dr Zoran Pavlović

Redovni profesor, Pravni fakultet, Univerzitet Privredna akademija u Novom Sadu
Pokrajinski zaštitnik građana - ombudsman

DECA I GOVOR MRŽNJE NA DRUŠTVENIM MREŽAMA

Mere protiv diskriminacije na međunarodnom i nacionalnom nivou, kao i uslovi korišćenja društvenih mreža, ne mogu u potpunosti da spreče širenje govora mržnje. Debata o pooštavanju sankcija protiv onih koji šire govor mržnje na društvenim mrežama, a gde se pojavljuju deca, treba da se vodi, ali i da se ne zaboravi pravo na slobodu govora i privatnost, standard efektivne zaštite prava decei drugo. Odgovornost snose svi, uključujući tu i društvene mreže. Prava deteta su neprikosnovena, kao i pravo na razvoj ili dostojanstvo. Zabrana pristupa društvenim mrežama deci nije preventivna mera, već vid nasilja nad njima, dodatna viktimizacijaa ne pozitivno-vaspitni mehanizam. Odgovoran pristup temi u trouglu govora mržnje, dece i društvenih mreža svoja rešenja neće se pokazivati kroz represivne mere kaznenog prava, već kroz prevenciju i stvaranje nulte tolerancije prema govoru mržnje na društvenim mrežama, bez obzira da li ga plasiraju odrasli ili deca.

KLJUČNE REČI: govor mržnje / društvene mreže / strategija zaštite prava dece / prevencija / nulta tolerancija

HATE SPEECH TOWARDS ROMA CHILDREN IN DIGITAL SPACE: DISCOURSE ANALYSES OF USERS' COMMENTS

Andrej KUBIČEK, MA¹
Aleksandra MARKOVIĆ, PhD²

The article explores new modes of textual articulation of long-existing discourses towards a specific segment of a racialized ethnic minority, the Roma children. Considering the interactive dynamic nature of digital media portals, which allows users to interact with media producers, algorithms, and themselves by posting comments, authors seek new ways to explain this phenomenon, which further endangers the precarious social position of the youngest Roma. The article shows how the hidden aspects of minority children's lives are fantasized in the texts (re)generated by the readers, who became producers of media messages through digital technologies. Besides centuries-old stereotypes and interpretations of selective everyday experiences about Roma children, the article points out how irresponsible and unethical journalism can encourage the emergence of hate speech towards a specific group of children already in a disadvantaged social position.

KEY WORDS: Roma children / discourse analyses / hate speech / digital media

¹ Research Associate, Institute of Criminological and Sociological Research in Belgrade, adrej.kubicek@gmail.com

² Research Associate, Institute of Criminological and Sociological Research in Belgrade, aleksandra.markovic1@hotmail.com

1. PUBLIC RECEPTION OF MEDIA'S REPRESENTATION OF CHILDREN

Themes concerning children have drawn the attention of the media reports since the very beginning of modern mass communications. It is almost paradigmatic to remember that one of the first waves of moral panic in 17th century Europe was caused by reporting about the fate of a boy belonging to an ethnic minority. Šimon Abeles, a twelve-year-old Jew from Prague, was allegedly murdered by the hands of his father in 1694. This event sparked the public's attention in many European countries, quickly fanning flames of anti-Semitic hatred (Marek, 2014).

Nevertheless, public awareness is not only quickly occupied by the texts in which children are depicted as victims. The same is true for reports in which children are stigmatized as those who commit a crime, mainly when such behavior is attributed to members of minority groups. Some authors rightly underline that traditional and digital media are essential for promoting and protecting children's rights (Pavlović, 2018: 93). On the other hand, empirical research in this field clearly shows that media reports about children, concretely about child labor, remain highly sensationalist (Stevanović, 2017).

The development of digital technologies has shaped a new symbolic reality of communication, comparable only to McLuhans' "Gutenberg galaxy" (McLuhan, 2011). Unlike Gutenberg's contemporaries, who have witnessed the democratization of the literary public (people who are able to receive messages), we are witnessing the democratization of authorship (ability to produce messages) (Prodanović, 2019: 205-206). Summarizing debates about the relationship between literacy and the development of digital technologies, authors in this field underline that its ever-evolving nature, which introduces new features and daily updates, means that actors need to adapt to those changes in order to remain competitive and use new means of communication efficiently, responsibly and productively (Stepanović, 2019: 47). These dynamic changes offer researchers an opportunity to understand better how readers qualitatively comprehend messages that mass media conveys to them, which was mainly hidden until now.

In the most extreme cases, such discourse articulations may represent hate speech, which is defined by its ability to incite hatred or prejudice towards a specific group; as a verbal act that threatens hostility, violence, discrimination, or exclusion; finally, hate speech slanders and stigmatizes whole groups (Kolaković-Bojović & Paraušić, 2020: 36). Also, it is essential to note that the Legislative in Serbia (Action plan for Chapter 23) recognizes the need to protect the rights of vulnerable groups among children, including Roma children in particular (Kolaković-Bojović, 2018: 177-178). Again, authors who have analyzed empirical aspects of this

problem emphasize that the (self) regulation of media is not working properly and that the Press Council is too weak, and social media operators do not prevent and eliminate hate speech (Müller, 2017: 18).

Having this in mind, the theme of this article is not only directed discrimination or concrete acts of hate crimes, speech, verbal violence, bullying, etc. It is also dedicated to reproducing unfavorable discourse, which forms the basis for further discrimination. This article's focus is thus discourse that jeopardizes children's rights and interests in the digital media space.

Racism in the digital environment can assume many different forms. On the one hand, it may be manifested in direct communication between users by taking forms of racist verbal/textual performances. This type of verbal manifestation of racism will not be tackled here because of the unavailability of material suitable for analysis, which usually remains hidden in private correspondences on the Internet³. The second form includes the production of the racist discourse in the digital format, again similar to "conventional" printed media texts. Analyses of these media reports show the steady disappearance of explicit racism toward Roma (particularly racist content about the children) and the presence of more indirect ways to convey messages about one's ethnicity and stereotypes tied to it (Kubiček, 2014; Kubiček, 2015).

This form of digital racism will be the primary focus of this article. First, as some authors show, non-Roma are usually unaware of the realities of Roma's private lives, including lives inside the family and childhood (Richardson, 2021), because they lack substantial social contacts. Following this assumption, it is highly improbable that adult non-Roma and Roma children have such communication by using digital channels of communication or that Roma children are reading media reports about their community and posted comments. This imbalance of power in virtual space, on the other hand, is mainly manifested through expertise in the use of modern information and communication technologies and the situational advantage that the abuser has over the victim (Milićević, 2021: 42).

2. DIGITAL PRACTICES OF HATE SPEECH

Discourse analyses focus not only on the content of the texts but also on modes that people employ in social communication. Digital technologies allow individuals, as was mentioned before, to employ text(s) as a practice, a way to perform

³ Still, one such case of private communication between two minors (one of them was Roma), ended in tragedy in 2010 and led to a racist pogrom in the village of Jabuka (Kubiček, 2022).

social actions (Jones, Chik & Hafner, 2015: 10). Namely, they can use narratives about Roma children to criticize institutions or specific cultural values; they can express their grievances, ask for protection, and claim moral or symbolic superiority. With this in mind, hate speech is far more than a manifestation of blind enmity. There is always more to it than it catches the eye in the first place.

Comments and media reports are intrinsically connected. For example, if the author of an article stresses ethnicity, the commentator will likely refer to it. Digital practices are interdependent, usually generated due to joint actions of individuals and bridging the gap between the physical and virtual world (Jones, Chik & Hafner, 2015: 3). Interaction is a new quality of discourse performance in the digital space, crucial for its understanding. This aspect of digital discursive practices can be understood in almost classical Mikhail Bakhtin's concept of dialogue (Bakhtin, 1981).

Some authors rightfully stress that perpetrators of digital violence – and racism is by definition closely tied with power struggles – usually remain anonymous. Also, once produced, such texts can remain present for a long time, which prolongs the victimization of individuals, or in this case, whole groups. Individuals who participate in such activities can remain unaware of the negative consequences they produce (Milićević, 2021: 42). This observation is hard to prove in our case study concerning the authors' anonymity and unavailability, but it leads to one crucial problem in the research. Namely, discourse analyses ought to explore different strategies for neutralizing racist verbal actions.

Also, those who use hate speech do so without fear of facing the consequences, despite legal mechanisms and specific policies of digital media which can prevent its promulgation (Kolaković-Bojović & Paraušić, 2020: 36).

3. ROMA CHILDREN AS SPECIFIC TARGET OF RACISM

Unlike the other stigmatized ethnic communities, whose members share the same dispositions regardless of their age or gender, Roma tends to be represented in more specific categories concerning mentioned dispositions. As Vesna Trifunović shows in the case of ethnic jokes, it is not unusual that Roma women and Roma children are presented as independent characters, sometimes being main actors in jokes on their own, unlike Jews, Germans, Banatians, Bosnian Muslims, etc. (Trifunović, 2009: 98). From the first literary depictions of the ancestors Roma, clear distinctions were made between age and gender groups. Still, these distinctions did not have an analytical function. Instead, they were used to reinforce general-

ly and profoundly negative perceptions, as Miguel de Cervantes describes in one of his novels: “Born of parents who are thieves, reared among thieves, and educated as thieves, they finally go forth perfected in their vocation, accomplished at all points, and ready for every species of roguery. In them, the love of thieving and the ability to exercise are qualities inseparable from their existence, and never lost until the hour of their death” (Cervantes, 1881: I). In the following centuries, many influential authors who wrote about Roma rarely failed to mention Roma children, representing them in a very unfavorable manner similar to Cervantes (Grellman; 1807; Lombroso, 1911). As in was already mentioned before, contacts between Roma and non-Roma are usually tied to specific places (streets, fairgrounds, marketplaces, taverns...) and concrete functions (crafts, entertainment, and other services). On the other hand, the private family life of Roma remains unknown to most non-Roma, who rarely visit their settlements and houses. Thus, it is not uncommon for prejudices to arise from this realm of unknown (Ćirić & Drndarević, 2019: 23).

Beyond these historically accumulated and deeply rooted stereotypes about Roma children, sociologists have described more realistic social conditions which affect their lives. Thus, it is crucial to understand these phenomena to explore further the discursive articulation of stereotypes and fantasies that form the basis of hate speech in the digital space.

First of all, in both sedentary and non-sedentary (now almost extinct nomadic groups), marriages were most commonly contracted between minors: girls around 12 to 13 years of age and boys who usually had 14 or 15 years. Only a tiny minority of better-off families would be able to leave their parents and establish a separate household. Others would live with their husbands’ parents as long as they were alive. Such households are deeply patriarchal, and the prevailing emotion among members is the expression of gratefulness for providing for life needs. Values concerning children also are transitionally different than in the surrounding society. Roma have the proverb that they love their children above all other things in life, which is a projection of clear indicators of one family’s success: having numerous, healthy and happy offspring. In this context, Roma families do not enforce strict discipline on their children in order to compensate for the harsh material realities (Mitović & Zajić, 1998: 60-61).

Studies about most deprived Roma children – those engaged in street economic activities⁴ – shows their striking exclusion from wider society. However, they

⁴ Which may include collecting secondary raw materials (paper, metal and plastics), as well as cleaning of car glasses, selling of petty goods or pauperly. Other psychically intensive services are not that common in larger urban centers. However, some older children do them as well: wood splintering, coal-carrying, clearing of basements and attics, or different kinds of help to green market sellers (bringing water, cleaning counters etc.).

are physically engulfed by it on the everyday level on a much larger scale and more visible than their non-Roma peers, who spend their time at home, in the kindergartens, at school and with their parents. Roma children's activities start early in the morning and last until around 5 pm. It is not hard to conclude that they do not have free time and cannot participate in important social activities like other children, which severely affects their life prospects. Both boys and girls collect secondary raw materials. If they are alone, they search in the vicinity of their homes, but if they go with their parents, the area they cover can be pretty significant. These children, in most cases, use some part of their earned money for their basic everyday needs. Life on the streets is harsh and unforgiving since it carries many hazards, such as injuries, compromised health due to weather conditions, and exposure to microorganisms. Concerning everything described until now, Roma children differ from their peers in many aspects (Simpson-Herbert et al., 2006: 69-78). Their social capital is lower than non-Roma, thus being deprivileged and ultimately more vulnerable to victimization (Pavićević & Bulativić, 2018: 296), which should be taken as the starting point in analyses of discursive representations of Roma children.

4. METHODOLOGY

The primary corpus of texts for discourse analyses are comments posted on digital media portals in Serbia concerning news about Roma children. Focusing on comments with elements of hate speech towards this particular segment of the minority population, only negative texts aimed directly at the children will be considered. Since such comments are relatively rare, a broader time frame must be covered, beginning from 2010 to this day (2022). That means that discourse analyses have total coverage of this particular type of digital text.

Still, most of the preliminary analyzed material shows that only a minor part of the comments are directed against children. Besides texts that show compassion for their fate or criticize institutions or society as a whole, most negative comments are aimed at parents.

A more detailed reading of data, which was done using search engines⁵, showed that most comments suitable to be included in the corpus come from

⁵ Applying both Google and portal search engines, authors searched for particular words. In the first phase of data collection, the phrase "Romani children" (*Romska deca*) was used. In the second phase, all articles tagged with the word "Roma" (*Romi*) were listed, and comments from those with children-related titles were included in the corpus.

two media portals: *Kurir* and *Telegraf*. Two more media portals, *Blic* and *Novosti*, contained one example, while most others (like *Politika* and *Danas*) did not have any data collection. That can mean that these portals have stricter policies of censoring hate speech or that their articles do not provoke malicious comments. For this reason, these two cases – *Kurir* and *Telegraf* – are chosen for they offer plenty of examples and rich qualitative data. Among them, only the most representative and illustrative examples are presented and analyzed in order to avoid repetition. Gathered material shows homogeneity, and the main themes are very compact and follow the same lines of argumentation. That made it easier to present them in the thematic order.

All comments are translated into English as precisely as they could be done. Some aspects of the original (writing mistakes, improper use of capital letters) could not be transcribed into presented English material. However, the original composition of texts and punctuation marks are followed closely.

5. DISCOURSE ANALYSES OF COMMENTS

5.1. Education

Children's education is the first topic that provokes hateful comments about Roma children. In one such text, reporting about the boycott of a school of non-Roma parents, one reader posted:

Let's ask the teachers in Padinska Skela how it is for them when the Roma who received free books interfere with their classes and other students, how it is when the same Roma curse them and attack them in front of other children and they can't do anything to them because they are protected like polar bears.⁶

The example clearly shows grievances towards “a system,” which is understood as unfair, yet the educational system is one of the places where Roma and non-Roma anecdotally meet. Also, the comment's author is arguing with the journalist, who does not approve actions of parents who segregate Roma children from their own. The interactivity of discourse performance can be noted in alleged hands-on experience, which is denied to the journalist and possibly to uninformed fellow readers. The actual content of presented stereotypes is well known: Roma (chil-

⁶ <https://www.telegraf.rs/vesti/srbija/2989445-skandal-u-bujanovcu-roditelji-ne-zele-da-im-deca-idu-u-skolu-sa-romima-oko-25-djaka-i-dalje-van-klupa/komentari/svi>, accessed on 12.4.2022.

dren) are supposedly aggressive and indecent, they jeopardize “normal” activities (learning) and are bestialized: compared with polar bears. A similar narrative can be found in the following example:

I work in a school that has Roma children. They always get free books and school accessories at the beginning that most of them don't even open. They get free snacks, excursions, and wardrobe packages ... Who forbids them to study? I can't say they don't have conditions.⁷

Here author informs the audience about her supposed professional life experience. Again, the notion that Roma children are unjustly favored (by getting free schoolbooks).

5.2. Begging

Begging is the theme that is the most extensively referred to in comments. As mentioned before, besides formal institutions such as schools, most readers come in contact with Roma in a very different, informal type of institution: the street. In the text from *Kurir* from 2014, which generated some of the most exemplar cases of hate speech, one reader is refereeing to his own everyday experience, with an emphasis on his physical bravery:

They want to spit on you and even throw stones at you, I stood in the protection of a girl at the station who pulled out 20 dinars and gave it to a little Roma girl, and then the others started attacking her and dragging her by the purse, and one.⁸

The stereotypical repertoire of this example shows the merging of begging, stealing, and aggressive and uncivilized behavior as the same thing. Still, there are topic quotations that emphasize only the begging, such as: *When you offer to buy them food, they refuse, they just want cash⁹, or Begging is their profession¹⁰.*

⁷ <https://www.telegraf.rs/vesti/srbija/2964751-tviter-gori-zbog-rasisticke-objave-rom-kinja-nije-morala-da-uci-jer-je-srpska-deca-ugrozavaju-ucenjem-pa-mora-da-bude-ravnopravna/komentari/svi>, accessed on 12.4.2022.

⁸ <https://www.kurir.rs/vesti/beograd/1165747/upozorenje-za-vozace-u-bg-romska-deca-se-bacaju-ispred-vozila-kako-bi-iznudila-novac/komentari>, accessed on 14.4.2022.

⁹ <https://www.kurir.rs/vesti/beograd/1165747/upozorenje-za-vozace-u-bg-romska-deca-se-bacaju-ispred-vozila-kako-bi-iznudila-novac/komentari>, accessed on 14.4.2022.

¹⁰ <https://www.kurir.rs/vesti/drustvo/2891827/uzasno-deca-prosjaci-su-zrtve-kriminal-aca-malisani-na-ulici-ni-zakonom-nisu-zasticeni>, accessed on 14.4.2022.

The narration of personal experiences can assume bizarre forms, as can be seen in the following example:

In Bor, I saw a little gypsy (ciganče) run out, and quite risky, in front of a bus carrying workers just to draw attention to a rather scantily clad “lady” (about 50 years old) who was huddled at that moment and threw out her tattooed “drumstick”... I have to admit that the scene was extremely comical, although when I think about it ... God, save me!¹¹

Details about the place, irony, and dramatic depiction of the event convince readers about the authenticity of the anecdote. The author summons the narratives from Charles Dickens’s novels about begging children involved in prostitution and shows them as a part of a broader marginalized milieu. A similar narrative is presented in the following illustrative comment, which contains echoes from the quoted Cervantes novel:

These children are victims of their parents who use them for begging from birth and later learn and force them to steal and harass innocent citizens. And we are their victims.¹²

Personal experience in the following case is narrated in order to draw the moral boundaries between “Us” and “Them”:

And I always wanted to buy them pastries in the bakery, they never wanted to, they just want money, that’s what they tell. When I once bought three pastries for them (they were in a group), they threw them at my feet.¹³

The person who wrote the comment stresses her compassion showed for children and her benevolent nature (“I always want to buy”), contrasted with their alleged arrogance and ungratefulness.

While sitting and eating in the restaurant, these small and slightly older Roma are harassing you, blackmailing you, hanging over your head, counting bites, showing crippled arms and legs, etc.¹⁴

¹¹ <https://www.telegraf.rs/vesti/beograd/1236736-decja-mafija-decaci-ubili-starca-opljackali-preko-300-gradjana-a-policija-im-ne-moze-nista-foto/komentari/svi>, accessed on 12.4.2022.

¹² <https://www.kurir.rs/vesti/drustvo/1618442/maja-gojkovic-deca-na-ulici-su-zrtve-a-ne-prestupnici/komentari>, accessed on 14.4.2022.

¹³ <https://www.kurir.rs/vesti/srbija/355139/tuzba-protiv-mekdonaldsa-zbog-diskriminacije-roma/komentari>, accessed on 14.4.2022.

¹⁴ <https://www.kurir.rs/vesti/srbija/329249/mekdonaldis-ispitacemo-slucaj-diskriminacije/komentari>, accessed on 14.4.2022.

The writer of quoted lines narrates his everyday experience in dramatic tones. Roma children are depicted as foreign and profoundly threatening to the pleasant scene of eating at the restaurant. This is achieved by addressing the public with “You,” implicitly meaning “Us,” who are trying to enjoy the meal, while “Them” poses an innate threat. Perceived injustice and strongly negative depiction of children are merged in the following example:

*If my child went somewhere naked and filthy, they would put me in a madhouse and him in a social institution! Right? That’s right!*¹⁵

“My child” here actually means “Our children” who are dressed and clean, while “We” are depicted as repressed and punishable by highly harsh measures.

5.3. Arraigned children marriages

Sensationalist reports that the patriarchal custom of child marriage is also a common trigger for elaborated hate speech. In the first example, the narrative is again used as a means of explaining generalized stereotypes about Roma children:

*Young Roma enters into sexual relationships. They get married young. The reason why young people get married? For a simple reason. You pay her, and she has to make that money. How? Well, theft, fraud, begging. Up to 18 years of age, she is not responsible for the committed acts because she is a minor.*¹⁶

Presented in the quasi-didactic form of questions and answers, the author reenacts the centuries-old narrative about supposed child slavery and employing children for criminal activities, which was mentioned before. “Us” and “Them” speech, with “normality” as a symbolic border between the two, can be noted in the following example:

*Well, her mother gave birth to her at 15 also, that is normal for them.*¹⁷

The final comment is also short yet proves to be very interesting for analyses:

¹⁵ <https://www.kurir.rs/vesti/srbija/328539/stop-za-male-rome-u-mekdonaldu/komentari>, accessed on 14.4.2022.

¹⁶ <https://www.telegraf.rs/vesti/srbija/3103969-romski-obicaji-o-braku-sa-devojcica-ma-jaci-od-zakona/komentari/svi>, accessed on 12.4.2022.

¹⁷ <https://www.telegraf.rs/vesti/svet/3104263-devojcica-12-rodila-bebu-ocu-20-preti-za-tvor-njena-majka-je-postala-baka-sa-27-godina/komentari/svi>, accessed on 12.4.2022.

*This should be punished. Parents to prison, and cubs to (juvenile detention) center. What is this, we are not in India and Pakistan.*¹⁸

The reader here does not try to inform others. Instead, he expresses his capacity to determine who should be punished. Again, we are witnessing the bestialization of Roma by using the word “cubs” (*mladunčad* in original) and strong Orientalist discourse in distancing from South Asian countries. The genetic connection between the countries of Roma ancestors’ origin and their present customs is a common strategy used to exoticize this minority.

5.4. Theft

Theft has already been registered as one of the most common stereotypical contents, sometimes inseparable from other similar depictions. In the following comment, thieving is referred to on its own:

*Does anyone ask how they can be such big thieves and how little they are??? Do you know what all these little ones do? How much they steal and cause damage, no one can do anything to them!!*¹⁹

The comment’s author raises moral panic by rhetorically posing a series of dramatic questions. The problem of minor theft is exaggerated and presented as an unsolvable problem. Supposed powerlessness or lack of will to solve this problem is also a common topic seen in most comments. Even more negative event narrated from personal experience is shared in the following example:

*I am personally afraid even of those little children!!! Three boys entered my shop, and each of them was holding a bag with glue. They were drugged and stole a cake and flew out!!!! And who should I complain to!!! Terrible, but everything is getting worse and worse...*²⁰

This comment is posted on the equally negative report titled *Monsters among us drug child beggars to earn money*. The media report itself is critical of adults

¹⁸ <https://www.telegraf.rs/vesti/srbija/2982074-buduce-mlade-imaju-najvise-13-godina-i-prodaju-ih-za-700-evra-i-boks-cigareta-sklapanje-decijih-brakova-u-srbiji-ne-prestaje/komentari/svi>, accessed on 12.4.2022.

¹⁹ <https://www.kurir.rs/vesti/srbija/329249/mekdonalds-ispitacemo-slucaj-diskriminacije/komentari>, accessed on 14.4.2022.

²⁰ <https://www.kurir.rs/vesti/drustvo/952851/monstrumi-medu-nama-drogiraju-de-cu-prosjake-da-bi-zaradili/komentari>, accessed on 14.4.2022.

who exploit children, but it causes strong emotions of fear in some readers. It is crucial to note the dehumanization of this particular group of children, as the context in which they are referred to is abnormal – adults typically aren't afraid of children. Emphasis on drug use adds to the grotesque picture in someone's workplace. As in the previous comment, the author also complains about his powerlessness because supposed child thefts are tolerated. The following example is particularly representative because it offers a more elaborated explanation of the analyzed topic:

*She must have put her hand in her bag; what kind of racism (you are talking about), gypsies try to get away with that, they steal as soon as they open their eyes.*²¹

The reader of the media article problematizing racism and violence against the children claims to know what really has happened, based on stereotypes that Roma girls steal. Stylistic diminishing of the act of beginning (“putting the hand in the bag”) should be understood as a sarcastic contrast to what follows – the claim that Roma supposedly steals from the very moment they are born (as an innate category). From the perspective of discourse analyses of racism, this example is paradigmatic. One fervently denies the racist nature of others' actions while simultaneously – literally in the same sentence – exhibits strong racist beliefs.

5.5. Aggressiveness

As the theft, the supposed aggressiveness of the Roma children was an essential part of the racist discourse repertoire in many previous examples. It is generally an essential topic in racism as an ideology. Threats are even more dramatic when supposed aggression is aimed at the other children, especially ones belonging to our group:

*I should beg the “little Roma” to stop harassing my child and robbing his money, and if I react immediately, it is on a national basis.*²²

The perceived injustice of this position is alleviated by irony (“I should beg”), plus we again find strong criticisms of the concept of minority rights, or at least of manipulations done with it. Some readers openly question ethical media standards:

²¹ <https://www.telegraf.rs/vesti/2518503-sahranjen-spaljani-beskucnik-njegova-decanisu-dosla-na-sahranu-ali-je-procitano-njihovo-pismo/komentari/svi>, accessed on 12.4.2022.

²² <https://www.kurir.rs/vesti/srbija/329249/mekdonalds-ispitacemo-slucaj-diskriminacije/komentari>, accessed on 14.4.2022.

*A burned man was buried, right? I didn't notice
you wrote "gypsy" for a little vandal.²³*

The following more extended quote corresponds with the negative title of the media report *Child mafia – boys murdered an older man and robbed over 300 citizens, and police can't do anything*:

They are killing the elderly, attacking pregnant women and you can't do anything, no. I can't believe it's happening in our country, don't you see that these children are mindless and that they should be sent to a madhouse and keep them there forever.. it's terrible to watch children kill, they attack the street and you can't do anything, so I can't believe in something like that, so as an older person I'm not sure if I can leave the house anymore or ?? !!!²⁴

The quoted text almost recapitulates many previously noted contents in almost an apocalyptic tone. The same sensationalistic title provoked one more comment which contains elements of extreme hate speech:

If they are not too young to do such things, they are not too young not to be responsible for them... So young and already a waste of society and should be removed from the streets.²⁵

6. CONCLUSION

Specific digital discursive practices in the case of Roma children show somewhat similar patterns as “non-digital” racist practices concerning this segment of the Roma population. They are an object of representation, unable to respond and express themselves. Although they are ever-present in the Internet’s verbally articulated fantasies of anonymous authors, these readers know very little about these children. In a sense, these children were virtual beings for them even before digital technologies. That can be explained by the considerable divergence between the

²³ <https://www.telegraf.rs/vesti/2518503-sahranjen-spaljeni-beskucnik-njegova-decanisu-dosla-na-sahranu-ali-je-procitano-njihovo-pismo/komentari/svi>, accessed on 12.4.2022.

²⁴ <https://www.telegraf.rs/vesti/beograd/1236736-decja-mafija-decaci-ubili-starca-opljackali-preko-300-gradjana-a-policija-im-ne-moze-nista-foto/komentari/svi>, accessed on 12.4.2022.

²⁵ <https://www.telegraf.rs/vesti/beograd/1236736-decja-mafija-decaci-ubili-starca-opljackali-preko-300-gradjana-a-policija-im-ne-moze-nista-foto/komentari/svi>, accessed on 12.4.2022.

physical presence of these children in an everyday street setting on the one hand; and the gaping hole of symbolic exclusion and lack of any communication and feeling of solidarity with them. They have not become pictures or video content on the screens. On the contrary – they were perceived like that in the first place.

The second finding is even more important since it points out the responsibility of media in the digital age. Analyzed data is compact and straightforward in the depiction of children and categories attributed to them. People who use hate speech are not members of extreme groups (Marković, 2013; Marković, 2015) and speak from the position of “normal,” “ordinary” people. They do not employ elaborated racist theories, quasi-historical argumentation, narratives about conspiracies, etc. Instead, they call upon their everyday life experience, common sense, and general beliefs. Individuals who write hateful comments are incited to do so by sensationalist reports. In the most analyzed cases, they were actually provoked to comment on events they consider to be unjust, regardless of the involvement of children. That calls for greater responsibility for journalists, who can fan hatred even if they do not explicitly reproduce negative narratives. Analyzed data clearly shows that bare mentioning of stigmatized groups in sensitive and contested topics and events can be harmful.

REFERENCES

1. Bakhtin, M. (1981) *Discourse in the Novel* (M. Holquist, & C. Emerson, Trans.). In: M. Holquist (Ed.), *The Dialogic Imagination*. Austin: University of Texas Press.
2. Cervantes, M. (1881) *The Little Gipsy Girl*. In: *The Exemplary Novels of Cervantes*, translated by Walter K. Kelly T.
3. Ćirić, J. & Drndarević, N. (2019) Migracije, strah, predrasude i manipulacije, *Zbornik Instituta za kriminološka i sociološka istraživanja*, 2/2019, pp. 19-34.
4. Grellman, H. M. G. (1807) *Dissertation on the Gipseys: Representing Their Manner of Life, Family Economy, with an Historical Enquiry Concerning Their Origin & First Appearance in Europe*, London: William Ballintine.
5. Kolaković-Bojović, M. (2018) Deca žrtve u Republici Srbiji: normativni okvir, reformski koraci i EU standardi. U: Stevanović, I. (ur.) *Pravda po meri deteta*, Beograd: IKSI, str. 171-184.
6. Kolaković-Bojović, M, Paraušić, A (2020a) Media Portrait of Drug Lords in Serbia, in: Miličević, M, Stevanović, I. *Drugs and Drug Addiction: Legal, Criminological, Sociological and Medical issues*. Beograd: IKSI, pp. 391-403.

7. Kolaković-Bojović, M, Paraušić, A (2020b) Hate Speech on Twitter: Attitudes Toward the Drivers of Electric Scooters. In: *Conference Proceedings Hate Speech and the Concept of Hate Crimes: Acts of Perception and Compulsory Social Conformism*, Bitola 11. November 2019. Bitola: Faculty of Law – Kicevo, University “St. Kliment Ohridski”, pp.35-51.
8. Кубичек, А. (2014) Дискурси о Ромима у дневној штампи. У: Недељковић Валић, Д. et al (ур.), *Улога медија у нормализацији односа на Западном Балкану*. Нови Сад: Филозофски факултет у Новом Саду, стр. 177-194.
9. Кубичек, А. (2015) Расизам према Ромима на интернету. У: Недељковић Валић, Д. et al (ур.), *Улога медија у нормализацији односа на Западном Балкану II*. Нови Сад: Филозофски факултет у Новом Саду, стр. 256-271.
10. Кубичек, А. (2022) Антициганистички погром у селу Јабука. У: Бакић, Ј. (ур.), *Истраживање национализма у Србији почетком 21. века*, Београд: Филозофски факултет, стр. 223-250.
11. Lombroso, C. (1911) *Criminal man, according to the classification of Cesare Lombroso*, New York: G.P. Putnam's sons.
12. Marek, T. (2014) *Veliká novina o hrozném mordu Šimona Abelese*, Praha: Argo.
13. Marković, A. (2013) Viđenje obrazovnog sistema i različita upotreba kulturnih sadržaja desnih i levih ekstremista u sajber prostoru Srbije, U: Jelinčić, J & Ilić, S. (ur.) *Politički ekstremizam u sajber prostoru Srbije*, Zrenjanin: CRCD, str. 89-100.
14. Marković, A. (2015) Odnos srbijanskih neonacista prema kapitalizmu: analiza neonacističkih web portala, blogova, foruma, Facebook-a i Twitter-a, in: *Sociologija*; Vol. LVII (2015), № 2, str. 380-400.
15. McLuhan, M. (2011) *The Gutenberg Galaxy*. Toronto: University of Toronto Press, Scholarly Publishing Division.
16. Milićević, M. (2021) Neke karakteristike sajber vršnjačkog nasilja i sajber viktimizacije u populaciji osoba sa ometenošću – pregled istraživanja, *Zbornik Instituta za kriminološka i sociološka istraživanja*, No. 2-3, str. 41-57.
17. Mitrović, A. i Zajić, G. (1998) Društveni položaj Roma u Srbiji. U: *Romi u Srbiji*, Beograd: Centar za antiratnu akciju i Institut za kriminološka i sociološka istraživanja.
18. Müller, S. (2017) *The Wall of Anti-Gypsyism Roma in Serbia*. Stockholm: CRD.
19. Pavićević, O. & Ilijić, Lj. (2018) Dobrobit dece i različiti oblici kapitala: socijalni, humani i kulturni kapital. U: Stevanović, I. (ur.) *Pravda po meri deteta*, Beograd: IKSI, str. 295-308.

20. Pavlović, Z. (2018) Zaštita privatnosti i dostojanstva deteta u medijskom prostoru. U: Stevanović, I. (ur.) *Pravda po meri deteta*, Beograd: IKSI, str. 91-102.
21. Prodanović, S. (2019) Između heterotopije i ideologije: o realnostima rijaliti programa u Srbiji. *Етноантрополошки проблеми*, н. с. год. 14 св. 1, str. 203-222.
22. Richardson, K. (2021) *Roma in the Medieval Islamic World: Literacy, Culture and Migration*. London: I.B. Tauris.
23. Simpson-Herbert, M et al. (2006) *Papirnati život*. Beograd: Otkrovenje.
24. Stepanović, I. (2019) Privacy and Digital Literacy: Who is Responsible for the Protection of Personal Data in Serbia? *Zbornik Instituta za kriminološka i sociološka istraživanja*, 3/2019, str. 45-56.
25. Stevanović, I. (2017) Najgori oblici dečjeg rada u Srbiji i izveštavanje medija. U: Stevanović, I. & Pavićević, O. (ur.) *Pravosuđe i mediji*. Beograd: IKSI, str. 209-238.
26. Trifunović, V. (2009) *Likovi domaćih viceva, Socijalni tipovi lude u savremenim vicevima*. Beograd: Srpski genealoški centar.

Online sources:

1. <https://www.telegraf.rs/vesti/srbija/2989445-skandal-u-bujanovcu-roditelji-ne-zele-da-im-deca-idu-u-skolu-sa-romima-oko-25-djaka-i-dalje-van-klupa/komentari/svi>, accessed on 12.4.2022.
2. <https://www.telegraf.rs/vesti/srbija/2964751-tviter-gori-zbog-rasisticke-objave-romkinja-nije-morala-da-uci-jer-je-srpska-deca-ugrozavaju-ucenjem-pa-mora-da-bude-ravnopravna/komentari/svi>, accessed on 12.4.2022.
3. <https://www.kurir.rs/vesti/beograd/1165747/upozorenje-za-vozace-u-bg-romska-deca-se-bacaju-ispred-vozila-kako-bi-iznudila-novac/komentari>, accessed on 14.4.2022.
4. <https://www.kurir.rs/vesti/beograd/1165747/upozorenje-za-vozace-u-bg-romska-deca-se-bacaju-ispred-vozila-kako-bi-iznudila-novac/komentari>, accessed on 14.4.2022.
5. <https://www.kurir.rs/vesti/drustvo/2891827/uzasno-deca-prosjaci-suzrtve-kriminalaca-malisani-na-ulici-ni-zakonom-nisu-zasticeni>, accessed on 14.4.2022.
6. <https://www.telegraf.rs/vesti/beograd/1236736-decja-mafija-decaci-ubili-starca-opljackali-preko-300-gradjana-a-policija-im-ne-moze-nista-foto/komentari/svi>, accessed on 12.4.2022.

7. <https://www.kurir.rs/vesti/drustvo/1618442/maja-gojkovic-deca-na-ulici-su-zrtve-a-ne-prestupnici/komentari>, accessed on 14.4.2022.
8. <https://www.kurir.rs/vesti/srbija/355139/tuzba-protiv-mekdonaldsa-zbog-diskriminacije-roma/komentari>, accessed on 14.4.2022.
9. <https://www.kurir.rs/vesti/srbija/329249/mekdonalds-ispitacemo-slucaj-diskriminacije/komentari>, accessed on 14.4.2022.
10. <https://www.kurir.rs/vesti/srbija/328539/stop-za-male-rome-u-mekdonaldsu/komentari>, accessed on 14.4.2022.
11. <https://www.telegraf.rs/vesti/srbija/3103969-romski-obicaji-o-braku-sa-devojcicama-jaci-od-zakona/komentari/svi>, accessed on 12.4.2022.
12. <https://www.telegraf.rs/vesti/svet/3104263-devojcica-12-rodila-bebu-ocu-20-preti-zatvor-njena-majka-je-postala-baka-sa-27-godina/komentari/svi>, accessed on 12.4.2022.
13. <https://www.telegraf.rs/vesti/srbija/2982074-buduce-mlade-imaju-najvise-13-godina-i-prodaju-ih-za-700-evra-i-boks-cigareta-sklapanje-decijih-brakova-u-srbiji-ne-prestaje/komentari/svi>, accessed on 12.4.2022.
14. <https://www.kurir.rs/vesti/srbija/329249/mekdonalds-ispitacemo-slucaj-diskriminacije/komentari>, accessed on 14.4.2022.
15. <https://www.kurir.rs/vesti/drustvo/952851/monstrumi-medu-nama-drogiraju-decu-prosjake-da-bi-zaradili/komentari>, accessed on 14.4.2022.
16. <https://www.telegraf.rs/vesti/2518503-sahranjen-spaljani-beskucnik-njegova-deca-nisu-dosla-na-sahranu-ali-je-procitano-njihovo-pismo/komentari/svi>, accessed on 12.4.2022.
17. <https://www.kurir.rs/vesti/srbija/329249/mekdonalds-ispitacemo-slucaj-diskriminacije/komentari>, accessed on 14.4.2022.
19. <https://www.telegraf.rs/vesti/beograd/1236736-decja-mafija-decaci-ubili-starca-opljackali-preko-300-gradjana-a-policija-im-ne-moze-nista-foto/komentari/svi>, accessed on 12.4.2022.

Andrej Kubiček, MA

Istraživač saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

Dr Aleksandra Marković

Istraživačica saradnica, Institut za kriminološka i sociološka istraživanja u Beogradu

GOVOR MRŽNJE USMEREN PREMA ROMSKOJ DECI U DIGITALNOM PROSTORU: ANALIZA DISKURSA KOMENTARA KORISNIKA²⁶

U radu se ispituju novi načini tekstualne artikulacije već dugo postojećih diskursa prema specifičnom segmentu rasijalizovane etničke grupe – romskoj deci. S obzirom na interaktivnu dinamičku prirodu digitalnih medijskih portala, koji objavljivanjem komentara korisnicima omogućavaju interakciju sa kreatorima medijskih poruka, algoritmima i sa drugim korisnicima, autori rada traže nove načine da objasne ovaj fenomen, koji dodatno ugrožava nesigurni društveni položaj najmlađih pripadnika Roma. Rad pokazuje kako se prikriveni aspekti života dece pripadnika manjinskih zajednica fantaziraju u tekstovima koje (re)generišu čitaoci, koji su putem digitalnih tehnologija postali i proizvođači medijskih poruka. Pored vekovnih stereotipa i tumačenja selektivnih svakodnevnih iskustava o romskoj deci, rad pokazuje na koji način neodgovorno i neetičko novinarstvo može da podstakne pojavu govora mržnje prema određenoj grupi dece koja su već u nepovoljnom društvenom položaju.

KLJUČNE REČI: romska deca / analiza diskursa / govor mržnje / digitalni mediji

²⁶ Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)

SOCIAL PEER VIOLENCE IN THE DIGITAL ENVIRONMENT - STUDENTS' ATTITUDES AND THE POSSIBILITY OF PREVENTION¹

Jelena KOSTIĆ, PhD²
Valentina RANALDI, PhD³

In recent years, communication between children and young people has increasingly taken place in the digital environment. A large number of minors have their own profile on social networks, as well as applications for exchanging phone calls and messages (e.g. Viber). As a result, their exposure to violence in the digital environment is increasing. This type of violence is specific, and the lack of direct contact can be encouraging for potential abusers. In addition, in some forms of digital violence, the reaction of the victimized person may be absent, and its absence may encourage further violence or even other forms of violence against him. During the pandemic caused by the COVID-19 virus, classes in schools were conducted online, and a measure of mandatory physical isolation was in force. This has certainly increased the use of social networks and messaging applications by children and young people.

Starting from the assumption that in that period children were more exposed to victimization by peers in the digital environment, from April to June 2021 we conducted two surveys through an anonymous survey among primary school students in the Republic of Serbia aged ten to fourteen. The aim of one research was to gain insight into students' attitudes and attitudes towards verbal peer violence in digital environ-

¹ The Introduction and the first chapter were written by Valentina Ranaldi and the second chapter and conclusion by Jelena Kostić.

² Senior Research Fellow, Institute of Comparative Law in Belgrade, j.kostic@iup.rs

³ Research Fellow, European Union Law, "Niccolo Cusano" University, Faculty of Law, Rome, Italy, valentina.ranaldi@unicusano.it

ments, and the other was to gain insight into students' attitudes and attitudes towards social peer violence in the same environment. This paper presents the results of another study. The basis for the assumptions from which we started were the researches of other authors, which we refer to in the first part of our paper. Based on the results of the research, we tried to give recommendations for the prevention of social peer violence in digital environments.

KEY WORDS: social peer violence / digital environment / prevention

1. INTRODUCTION

There are numerous definitions of bullying. According to the Committee on Education and Skills of Great Britain, it means behavior that is harmful to mental and physical health and includes: insults, provocations, ridicule, giving malicious comments, hitting, pushing, taking property (things), inappropriate texts via messages and emails, sending offensive and degrading photos over the phone or the Internet, gossiping, removing people from the group and spreading false and harmful rumors (Bullying, House of Commons, Education and Skills Committee, The Stationery Office, London, 2007: 8, stated according to Đorić, 2009: 148).

According to authors, a large number of studies on peer violence in European countries and the United States have long concluded that victimization of victims of peer violence has negative consequences on school success and daily functioning, personal experience and academic achievement. In addition, victimization often contributes to anxiety, depression, anxiety, feelings of loneliness, fear, and helplessness (Donoghuea *et al*, 2014: 41).

In recent years, more and more attention has been paid to the study of the phenomenon of cyberbullying, as a behavior undertaken through electronic or digital media (email, mobile phones or social networks). Some authors believe that this type of violence is undertaken by repeating a certain pattern of behavior in an attempt to harm a person (Ortega *et al*, 2012, p. 323, stated according to Navarro, Yubero, Larañaga, 2015: 2). However, we are of the opinion that children of a certain age (aged 10 to 14) are often not even aware of the damage they can inflict on their peers by such behavior, and that is why they easily undertake activities that can be classified as social peer violence.

Some authors believe that cyberbullying is a specific type of social violence perpetrated through digital media (Beran and Li, 2007, stated according to Navarro *et al*, 2015: 16). However, the very nature of cyberbullying is such that it mainly in-

volves verbal or social violence. Although it may seem at first that such behavior does not cause as much damage as physical violence, its consequences can be very serious and long-lasting, especially when it comes to children. Such behavior can greatly impair a minor's self-confidence and negatively affect his or her future personal and professional achievements.

Increased violence in the digital environment is certainly due to its characteristics, which include the possibility of anonymity of the perpetrator, greater public exposure than when the violence is committed live, the inability to be excluded from the cyber environment and the lack of contact in many types of traditional violence. Some adolescents think that by taking on activities that can be classified as cyberbullying, they find themselves with their peers, unaware of the seriousness of the negative consequences of such behavior (Ferara *et al*, 2018: 2).

According to research, people who are victims of conventional violence very often become victims of violence in the digital environment. Likewise, people who are violent in the real (physical environment) very often become violent in the digital environment as well. However, the fact that people who were not previously prone to violence in the real (physical) environment are often violent in the digital environment (Låftman *et al*, 2013: 112)

As stated in the research conducted in Sweden, violence in the digital environment causes the same consequences in adolescents as conventional violence. These include psychosomatic problems of victims of violence, depression, anxiety, feelings of loneliness, lower levels of self-confidence, lower levels of academic success, substance abuse, propensity to self-harm, as well as suicidal ideation and suicide attempts. The highest levels of psychological stress caused by digital violence have been reported in children, who are often very exposed to this type of violence (Fridh *et al*, 2015: 2).

However, a special problem is the great availability of social networks for children. Thus e.g. the most popular social network Facebook does not take into account the age of the person who opened the user account. According to the company's policies, a person who opens his own account must be at least thirteen years old at the time of its opening, but this is not verified and is not subject to any restrictions or sanctions if a minor reports false information. If it is a younger person of the stated age, whether or not that person will use social networks is decided exclusively by the parents, who can report such a circumstance to Facebook by filling out an electronic form to terminate the minor's user account (Kostić, 2017: 430, Diligenski and Prlja, 2014: 33-34). Nevertheless, due to the great availability of social networks, frequent peer communication both through them and through applications for the exchange of telephone calls and messages, it is increasingly difficult to control the activities of children in the digital environment. It seems that

the school is often powerless to prevent peer violence in digital environments, although there are legal mechanisms for the prevention and sanctioning of behavior that violates the dignity, and sometimes the health and development of minors. A special problem is the fact that today more and more young minors are starting to use social networks and applications for exchanging calls and messages, which is why in our work we started from the assumption that a large number of children aged 10-14 have their own profile on social networks and applications. call and message exchange, and that they are often unaware of the consequences of their behavior in the digital environment.

In order to prevent all types of peer violence, especially the one that takes place in the digital environment, the awareness of both students and teachers should be raised, school rules on combating peer violence should be reviewed and, if necessary, improved, and adequate programs should be implemented. reduction of peer violence (Batori *et al*, 2020: 106).

2. SOCIAL PEER VIOLENCE, DEFINITION AND APPROACH IN THE REGULATIONS OF THE REPUBLIC OF SERBIA

Schools and parents have a great role in teaching children, but the environment which also consist of peer people, contributes to a great extent to the formulation of personality. The desire to accept and belong to a certain group often directs the behaviour of individuals. If certain behavior is unacceptable, it should be prevented from repeating it and the minor should be pointed out the consequences of their own mistakes, because children at a certain level of psychophysical development are not aware of the possibility of their occurrence or their seriousness.

The Law on the Fundamentals of the Education System provides for the right to protection from discrimination and violence, abuse and neglect. In addition, it prescribes obligations. Serious violation of obligations under the provisions of the said law also includes the use of mobile phones, electronic devices and other means for purposes that endanger the rights of others (Article 83, paragraph 2, item 7 of the Law on The Fundamentals of the Education System, *The Official Gazette of the Republic of Serbia*, no. 88/2017, 27/2018-other law, 10/2019, 27/2018-other law, 6/2020 and 129/2021). As far as the educational institution itself is concerned, physical, mental, social, sexual, digital and any other abuse of student violence is prohibited in it (Article 111, paragraph 1). Unlike previous regulations, the Law on the Fundamentals of the Education System prescribes the definition of digital violence and abuse. It refers to the misuse of information and communication technologies that can result in injury to another person and en-

dangerment of dignity by sending messages by e-mail, SMS, MMS, via the website, chatting, joining forums, social networks or other forms of digital communication (Article 111, paragraph 3).

According to national regulations governing education, violence and abuse means any form of once committed or repeated verbal or non-verbal behavior that results in actual or potential endangerment of the health, development and dignity of the child and student or employee.⁴ In addition to the definition of violence, the Rulebook on the Protocol of Actions to be taken by institutions in response to bullying, abuse and neglect recognizes social and digital violence as special types of violence. Social violence is considered to be behavior that excludes children and students from the group of peers and various forms of social activities, separation from others, non-acceptance on the basis of diversity, denial of information, isolation from the community, denial of social needs. Digital violence and abuse means the misuse of information technology, which can result in the injury of another person and endangerment of dignity. It is realized by sending messages by e-mail, SMS, MMS, via a website (web site), chatting, joining forums, social networks and the like. When we talk about social violence in the digital environment, we mean a social combination of these activities, which are reflected in the expulsion of peers from chat groups, denial of responses to their messages within chat groups, social networks and messaging applications. Bearing in mind that social interaction is increasingly taking place in digital environments, social violence is becoming more and more present on social networks and applications for the exchange of calls and messages.

In accordance to the Rulebook on the Protocol of Actions to be taken by institutions in response to bullying, abuse and neglect should be contributed by both education staff and parents, as well as students themselves. The obligation of the school is to acquaint all employees, children, students and parents with their rights, obligations and responsibilities, prescribed by law, the Rulebook on Protocol and other bylaws and general acts. In the case of the class community, according to the Rulebook, the class teacher, educator, teacher and professional associate should contribute to the acquisition of quality knowledge and skills, as well as the formation of values for mutual understanding, respect for diversity, constructive conflict resolution, etc. Therefore, in our research, we started from the assumption that it is necessary to organize lectures for students on the prevention of peer violence, which will be adapted to their age and needs.

Employees in the school institution must not provoke or contribute to violence, abuse and neglect (eg disrespect for the person and rights of the child and

⁴ The Rulebook on the Protocol of Actions to be taken by institutions in response to bullying, abuse and neglect, *Official Gazette of the Republic of Serbia*, no. 46/2019 and 104/2020.

students, inconsistency in behavior, biased assessment, etc.). It is this teacher behavior or attitude that can contribute to different types of violence by other students. In addition, students are also obliged to respect and honor the personality of other students, provide support to peers, contribute to and participate in prevention activities, and their behavior does not provoke, contribute to, or participate in violence or abuse. The rulebook prescribes the manner in which the school reacts to the different levels of violence that are undertaken against students, and the measures that are taken depend on the degree of threat to the rights and interests of students.

However, a particular problem may be how to respond to social violence in the digital environment. This type of violence often goes unnoticed, because students, even though they have been exposed to such violence, do not report it, because they believe that they will be able to overcome the problem on their own. However, we believe that this type of violence, as well as any other, should be openly discussed. If others are aware of the consequences it can have on the individual, they may refrain from such behavior.

3. BASIC RESEARCH DATA

Starting from the assumption that students focused on the use of digital technologies and communication via mobile phones, especially after the coronavirus pandemic, as well as the assumption that they are often unaware of the consequences of their actions and therefore need additional education in the prevention of peer violence, during 2021, we conducted a two-part survey. The first part of the research was conducted to find out the attitudes of students towards verbal peer violence in the digital environment, and the second part, which was also specific, referred to non-verbal peer violence in the digital environment.⁵ Having in mind the most frequent type of peer violence that is carried out in that environment in a non-verbal way, the subject of the research was primarily social violence. Our research is conducted among primary school students, aged 10 to 14, bearing in mind that a large number of students have been using social networks and applications for exchanging phone calls and messages since the age of 10. Research was of the survey type, and the questions were limited to social peer violence in the digital environment. In order to get as honest answer, our survey was anonymous.

⁵ The results of the first part of the research on the attitudes and attitudes of primary school students towards verbal peer violence in digital education were published in Kostić, J. (2021), Stavovi i odnos učenika prema verbalnom vršnjačkom nasilju u digitalnom okruženju, *Sociološki pregled*, vol. LVI, no. 4, pp. 1696–1718, doi: 10.5937/socpreg55-34445.

3.1. Research sample

About 500 primary school students from the territory of the city of Belgrade, Smederevo, Kragujevac and Novi Becej participated in the research. The research was based on the assumption that children from the fourth grade start using mobile phones and applications for exchanging phone calls and messages, as well as that children aged 10 to 14 are mostly unconscious as a consequence of their actions.

3.2. Research period

The research was conducted in the period from April to June 2021, together with the research on students' attitudes towards verbal peer violence in the digital environment. This was preceded by the last cycle of online classes. Given the limited possibility of physical contact with peers, we thought that to that extent there may have been a greater possibility of social violence in digital environments, because at that time students' communication via telephone and social networks was increased. That is why we were especially interested in the attitude of students towards this type of violence.

3.3. Research aim

The aim of our research was to obtain data, ie to gain insight into the attitude and attitude of primary school students in the territory of the Republic of Serbia towards social peer violence in the digital environment. As well as when it comes to researching students' attitudes and attitudes towards verbal peer violence in the digital environment, we sought to find out the feelings of people who have experienced this type of violence, their attitudes towards other peers who have experienced it, attitudes about the need for training. attitude about how much they benefited from the conducted trainings in the field of prevention of this type of peer violence. Based on the results of the research, we tried to give recommendations for its prevention.

3.4. Hypotheses

The research assumes that a large number of children aged 10 to 14 have a profile on social networks and applications for exchanging phone calls and messages, as well as that they do not understand the consequences of this type of violence, so they do not take the problem seriously. One of the assumptions is that children

need additional education to prevent social violence in the digital environment in order to know how to react in certain situations and to influence the prevention of behavior of their peers who exclude individuals from groups on social networks or applications for exchange of telephone calls and messages.

3.5. Research results and analysis

The results of the research show that the largest number of children aged ten to fourteen have their own profile on social networks (72.9%), while 27.1% of respondents do not have a profile on them. This supports the initial assumption that a large number of children of that age have a profile on social networks. The highest percentage of respondents 64.1% have a profile on the social network Instagram, followed by Tik Tok 53.2% and Facebook 21%. The smallest number of respondents, 5.5%, have a profile on the social network Twitter. Of the total number of respondents, only 5.2% do not have a profile on applications for the exchange of telephone calls and messages. The largest number of respondents, 88.7%, have a profile on the Viber application, followed by 49.7% on Votstap, and 3.2% on Telegram.⁶

According to the answers of the respondents, the largest number of them, 73.5%, never expelled a friend from the group on the application for understood messages, a total of 22.6% did so as the group administrator, while a smaller number 3.9% stated that they do not use applications for messaging.

Excluding 70.6% of students who stated that they had never expelled a friend from the group within the call and message exchange applications, a total of 5.5% of students who said they did not use the messaging application, in total 18.7% of respondents said that they did it because they believe that he or she does not belong there and that they should not be part of that group, 4.2% of respondents said that they did it so that they could talk about him or her other members of the group could talk about what the expelled person should not hear, while 3.2% of respondents said that they wanted to humiliate the expelled person in this way. This is exactly what testifies to the danger and possibility of increasing the intensity of social violence. A person who has been expelled from the group may not only feel isolated because of that act, but his peers may tell various untruths or ridicule some of his traits, and because of such isolation he may be unable to defend himself. Later, this type of violence can turn into verbal or even physical violence.

⁶ The same question was used in the research of students' attitudes and attitudes towards verbal peer violence in the digital environment, and the results of which were published in the paper, Kostić, J. Stavovi i odnos učenika prema verbalnom vršnjačkom nasilju u digitalnom okruženju, p. 1702.

In addition, it can be concluded that the motives for expelling peers from the call and message exchange group were still negative. Based on this, it can be concluded that although they are often unaware of the consequences of their own behavior, social violence is not the result of ill-considered actions.

If we ignore the number of 67.1% of respondents who never expelled a friend from the messaging group as an administrator, as well as 5.5% of students who do not use messaging applications, a total of 20% of respondents who did so said that none of the members of the group criticized them for such an action, and 7.4% that they were criticized by other members of the group. It is surprising that a larger number of students do not defend a person against whom a certain type of violence is committed, regardless of the fact that social violence in the digital environment is the work of an individual (group administrator). It is possible that he is a dominant member of a peer group who is most often opposed by other students in a real, school environment.

A total of 68.1% of students stated that they had never expelled a friend from the group for exchanging calls or messages, and 5.5% of students did not use such applications. Of the total number of students who expelled a friend as an administrator within the group for exchanging calls and messages, a total of 19% of students said that it did not affect the attitude of other students towards him, 4.2% said that after In addition, a large number of children or most did not want to hang out with a person who was expelled from the group within the application, while 3.2% of respondents said that even before being expelled from the group, no one wanted to hang out with that student. Therefore, it does not necessarily mean that social violence is always undertaken against students who have already been exposed to this type of method. It is possible that such an activity is undertaken with the aim of further excluding an individual from a peer group.

When it comes to the frequency of expelling students from the application for exchanging calls or messages, a total of 48.7% of students said that it happens, but not so often, 31.6% of respondents said that it does not happen at all, 14.5 % that it happens often, and 5.2% of students that they cannot answer that question because they do not use applications for exchanging calls and messages. group.

Out of the total number of participants in this research, a total of 63.2 respondents stated that they would never be expelled from the group within the application for exchanging messages or calls, 31% stated that they were expelled from that group, and 5.8% that they did not profile within such applications. More students appear to have declared themselves victims of social violence in digital environments than have admitted to committing this type of violence. This can be a consequence of self-blame. However, the question may be asked whether a certain number of students would undertake such an activity if they were not only aware

of the possible consequences of such behavior, but also the fact that it can be characterized as social violence.

If we ignore 59.7% of respondents who said they were not previously expelled from the group in the application for messaging or calls and 5.5% who said they do not have a profile within them, 24.6% of respondents said that the expulsion did not affect the attitude of other students towards him, 5.8% said that such an action had a negative impact on the attitude of other students towards him, who began to avoid it, while 4.2% of students said that the attitude he did not change other students towards him because that attitude was bad even before that.

Of the total number of respondents, excluding 62.8% of surveyed students who stated that no one has excluded them from the application for the exchange of calls and messages and 5.5% who stated that they do not have a profile within such an application, a total of 18, 4% of respondents were completely indifferent to the fact that their peers excluded them from the group within the said application, 5.5% of respondents felt great anxiety and discomfort, 4.8% of respondents thought about it for a long time, and 3.2% it felt less valuable than other peers. Based on that, it can be concluded that different individuals of the same age react in different ways to social peer violence, so it is possible that they may have different consequences as a type of long-term reaction to this type of violence. That is why preventive measures must be taken by individuals to prevent such behavior. This is exactly what the education that should be conducted regularly at the level of the educational institution can help.

Despite different answers and attitudes towards other people's and one's own victimization, a total of 44.2% of respondents believe that there is more violence on social networks and messaging applications than live, 36.8% believe that violence is equally present on social networks and schools, and 19 % that it is more represented in school, during direct socializing. Regardless of the fact that young people are spending more and more time in the digital environment, it can be concluded that they are still aware of the growing exposure to peer violence on social networks. This is a signal that continuously the necessary measures are being taken to prevent them from becoming victims themselves or from undertaking activities that can be characterized as social violence.

Having in mind the different attitudes of the respondents towards social violence in the digital environment, we were interested in how they evaluate the previous trainings related to education on peer violence on social networks. A total of 39.4% of respondents said that the trainings were very useful, 11.9% of respondents that they were completely useless, and 39.4% that they were very useful, but that they should be adapted to their needs and age. This suggests that the approach to the prevention of peer violence should be more comprehensive. The extent to which social violence in digital environments is present in schools should be ex-

amined first, and then a strategy for its prevention should be developed at the level of each institution. This does not have to be part of a specific assessment or strategy, but it should certainly be emphasized that peer violence in the digital environment requires special, specific and continuous approach.

4. CONCLUSION

In our research, we started from the hypothesis that a large number of students aged 10-14 have their own user profile on social networks and applications for exchanging phone calls and messages. The results of the research confirm that assumption. Most children of this age not only have their own user account on them, but also have several user accounts on various social networks (e.g. Instagram, Tik Tok or Facebook). This also increases their exposure to peer violence on social networks, as well as the possibility of victimizing others. Social violence in the digital environment is also present, and the exclusion of peers from the group within telephone and messaging applications increases the possibility of their further victimization, as they are often excluded from them in order to talk negatively with other peers. Although primary school children are often unconscious of the consequences of social violence against other peers, they always have a motive for doing so. According to the answers we received during the research, these motives are not harmless at all. Peers are mostly socially isolated in the digital environment in order to humiliate themselves in front of others or to say negative things about them to other people in the peer group. This is exactly what can encourage further violence, as well as other forms of violence against a person who has been exposed to this type of victimization. Students react very differently to social violence in the digital environment. It seems that a very small number of peers are defending the person against whom such activity was undertaken. The reason for this may be twofold. The first is the lack of awareness that such behavior is a form of violence that can have very serious consequences for some peers, and the second reason is the desire to be part of a group and to please the will of peers who have taken an activity that can be characterized as social violence. are often someone who imposes their will.

According to the results of the research, students believe that violence is more present in digital environment than in school. The reason for that is the fact that children spend more and more time using computers and mobile phones, and less socializing live. The physical isolation caused by the pandemic caused by the COVID-19 virus additionally contributed to all that.

Lack of understanding of the problem of social peer violence in the digital environment can also be caused by a lack of awareness of its harmfulness. It is possible

that some of the juveniles are not even aware that such behavior can be characterized as violence, so they would refrain from these activities if they knew that they could be labeled as bullies. Although, in our opinion, it is not possible to completely prevent social peer violence in the digital environment, we believe that the education of minors would significantly contribute to its prevention. According to the results of our research, the respondents rated the trainings they attended in the previous period, regarding digital violence, as very useful. However, they should be more comprehensive and include different forms of violence in both real and digital settings. In addition, in their opinion, they should be as adapted as possible to their age and needs.

REFERENCES

1. Batori, M., Ćurlin, M. and Babić, D. (2020) Nasilje putem interneta među adolescentima, *Zdravstveni glasnik*, vol. 6, no. 1, 104-114.
2. Beran, T., and Li, Q. (2007) The relationship between cyberbullying and school bullying, *Journal of Student Wellbeing*, no. 1, pp. 15-33.
3. Diligenski, A. and Prlja, D. (2014) *Fejsbuk i pravo*, Belgrade: Institute of Comparative Law.
4. Donoghuea, C. Almeida, A., Brandwein, D., Rochac, G. and Callahana, I. (2014) Coping With Verbal and Social Bullying in Middle School, *The International Journal of Emotional Education*, vol. 6. no. 2, pp. 40-53.
5. Đorić, M. (2009) Buling kao vrsta socijalnog nasilja, *Politička revija*, no. 3, pp. 145-164.
6. Ferrara, P., Ianniello, F., Villani, A. and Corsello, G. (2018) Cyberbullying a modern form of bullying: Let's talk about this health and social problem. *Italian Journal of Pediatrics*, 44(14): 1-3.
7. Fridh, M., Lindström, M. and 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*, 15:949, pp. 1-11, DOI 10.1186/s12889-015-2239-7.
8. Kostić, J. (2017) Posting Children's photographs on social networks: Sociological and legal aspects, *Sociološki pregled*, vol. LI, no. 3, pp. 413-433. doi:10.5937/socpreg51-15397.
9. Kostić, J. (2021), Stavovi i odnos učenika prema verbalnom vršnjačkom nasilju u digitalnom okruženju, *Sociološki pregled*, vol. LVI, no. 4, pp. 1696-1718, doi: 10.5937/socpreg55-34445.

10. Låftman, S.B., Modin, B., Östberg, V. (2013) Cyberbullying and subjective health. *Children and Youth Services Review*, 35(1): 112-119.
11. Navarro, R., Ruiz-Oliva, R., Larrañaga, E. and Yubero, S. (2015) The Impact of Cyberbullying and Social Bullying on Optimism, Global and School Related Happiness and Life Satisfaction Among 10-12 year old Schoolchildren, *Applied Research in Quality of Life*, 10, pp. 15-36, <https://doi.org/10.1007/s11482-013-9292-0>.
12. Ortega, R., Elipe, P., Mora-Merchán, J. A., Genta, M. L., Brighi, A., Guarini, A., Smith, P.K., Thompson, F., and Tippett, N. (2012) The Emotional Impact of Bullying and Cyberbullying on Victims: A European Cross-National Study, *Aggressive behavior*, 38(5), pp. 342-356.
13. The Law on The Fundamentals of the Education System, *The Official Gazette of the Republic of Serbia*, no. 88/2017, 27/2018-other law, 10/2019, 27/2018-other law, 6/2020 and 129/2021.
14. The Rulebook on the Protocol of Actions to be taken by institutions in response to bullying, abuse and neglect, *Official Gazette of the Republic of Serbia*, no. 46/2019 and 104/2020.

Dr Jelena Kostić
Viša naučna saradnica, Institut za uporedno pravo

Dr Valentina Ranaldi
Naučna saradnica, Pravni fakultet Niccolo Cusano, Rim, Italija

SOCIJALNO VRŠNJAČKO NASILJE U DIGITALNOM OKRUŽENJU – STAVOVI STUDENATA I MOGUĆNOST PREVENCIJE

Poslednjih godina komunikacija dece i mladih se sve više odvija u digitalnom okruženju. Veliki broj maloletnika ima sopstveni korisnički nalog na društvenim mrežama, kao i aplikacijama za razmenu telefonskih poziva i poruka (npr. Viber). To utiče na povećanje izloženosti različitim vrstama nasilja u digitalnom okruženju u kojem nedostatak direktnog kontakta sa žrtvom može biti ohrabrujući za potencijalne nasilnike. Osim toga, u nekim oblicima digitalnog nasilja, reakcija viktimizovane osobe može izostati, a njeno odsustvo može podstaći dalje nasilje ili čak druge oblike nasilja nad njom. Tokom pandemije izazvane virusom COVID-19, nastava u školama se odvijala online, a na snazi je bila i mera obavezne fizičke distance, pa čak u nekim situacijama i izolacije. To je uticalo na povećanje korišćenja društvenih mreža i aplikacija za razmenu telefonskih poziva i poruka od strane dece i omladine.

Polazeći od pretpostavke da su u tom periodu deca bila u većoj meri izložena vršnjačkom nasilju u digitalnom okruženju, od aprila do juna meseca 2021. godine sproveli smo dva istraživanja putem anonimne ankete među učenicima osnovne škole, uzrasta od 10 do 14 godina. Cilj prvog istraživanja bio je uvid u stavove studenata o verbalnom vršnjačkom nasilju u digitalnom okruženju, a drugog uvid u stavove studenata prema socijalnom vršnjačkom nasilju u istom okruženju. U ovom radu predstavljeni su rezultati drugog istraživanja. Svoje pretpostavke zasnovali smo na istraživanjima drugih istraživača koja su sprovedena u prethodnom periodu, a na njih se i pozivamo u našem radu. Na osnovu rezultata istraživanja pokušaćemo da damo preporuke za unapređenje prevencije socijalnog vršnjačkog nasilja u digitalnom okruženju.

KLJUČNE REČI: socijalno vršnjačko nasilje / digitalno okruženje / prevencija

CYBERBULLYING AS A FORM OF PEER VIOLENCE IN SCHOOLS

Nebojša MACANOVIĆ, PhD¹
Ružica STOJANOVIĆ, MA²

Violence by the means of the Internet, known worldwide as cyberbullying, is a general term for any communication activity using cyber technology that could be considered harmful to the individual or the common well-being. An increasing number of children and young people are being exposed to bullying via the Internet and additionally, the fact that it is still not recognized as a serious problem in society is worrying. One of the reasons why this trend is neglected lies in the fact that it occurs in the virtual world, and that it is not present in the “the real environment” of a child. The goal of this paper is to display empirical research that aims to determine the presence and the manner of cyberbullying among students in high schools in the municipality of Modriča, as well as the connection of this phenomenon with the educational and demographic characteristics of respondents. The research focuses on students and school as a place where these problems are often identified in young people. The results of the research indicate the existence of cyberbullying, but also reveal the causes and consequences of this phenomenon.

KEY WORDS: violence / cyberbullying / internet / social networks, school.

¹ Associate Professor, Faculty of Political Sciences, University of Banja Luka, nebojsa.macanovic@fpn.unibl.org

² Daycare for Children with special needs “Sunce Oberwallisa“, Modriča, stojanovicruzica7@gmail.com

1. INTRODUCTION

This world is filled with the intense development of information and communication technologies, and each individual can quickly and easily access the Internet, computers, mobile phones, and social networks. Today, the Internet has become more accessible and offers more and more services used by more and more people, both the young and the adult (Karamazan, 2016). The use of the Internet has significantly influenced the development of young people. That is, the growth of social networks on the Internet, as a new form of communication, significantly influences the development of the personality of children and young people (Dimitrijević, 2018).

Digital devices and media are a part of our everyday life. New generations today are growing up with digital media and technology. Children spend most of their time with the media, and through various content, they acquire new knowledge, and learn about values, opinions, and patterns of behaviour (Osmančević, 2016). Children and young people are continuously surrounded by information and communication technologies and start using them very early. There is a huge potential and many benefits of modern technologies, provided that they are used smartly, conscientiously, and moderately (Macanović, Bobrek Macanović, 2021).

However, there are some negative aspects to the development of new communication means, one being the appearance of Electronic Aggression or Cyberbullying. The most common types of cyberbullying occur through social networks because they are the most widespread phenomenon today. Social networks are very suitable for aggression, because they enable users to negatively comment and insult others, and allow such negative information to spread at high speed (Miladinović, Petričević, 2013). Among the most famous and popular social networks are Facebook, Instagram, Twitter, YouTube, Blog, TikTok, etc. Social networks enable children, young people, and adults to share their thoughts and ideas with the general public, but also to spread hatred towards others (Ciboci, 2014).

2. THE CONCEPT AND CHARACTERISTICS OF CYBERBULLYING

Changes in society and the era of the development of information and communication technologies bring about negative phenomena and many dangers. One of

these phenomena is a new type of violence - cyberbullying or bullying committed through the Internet and social networks (Mandarić, 2012). In addition to this problem, other dangers appear on the Internet, such as paedophilia, abuse, blackmail and others (Miliša, 2012). The Internet carries with it many risks and harms, especially for the most vulnerable groups of users, namely children and young people. People on the Internet and social networks can easily hide their identity, they do not have too much responsibility for the spoken word, they can create a false sense of security, etc. (Osmić, Čustović, 2018). Cyberbullying can be seen as sending or posting offensive images or texts via the Internet or other digital means of communication. It can also be harassment by phone calls, harassment on social networks, as well as harassment via SMS messages. In practice, students who already have conflicts with other students, who either have abused or have been abused, and those who use psychoactive substances are at a higher risk of being victims or perpetrators of cyberbullying (Jugović, 2018).

Besides Electronic Aggression, cyberbullying includes harassment via mobile phones. Harassment via mobile phone is any form of message (text, video, or photo), i.e. multiple messages a bully sends to threaten or inflict a feeling of discomfort on the victim. It can be seen today that almost every child owns and uses a telephone, even though children are not always able to distinguish appropriate from inappropriate content, thus increasing the possibility of sending and receiving violent messages, calls, and other content (Špigl, Žakula-Desnica, Bubnić, 2010).

In addition, Electronic Aggression among the young can be seen as a modern form of peer violence that is carried out through the media, i.e. the Internet and mobile phones, with the aim of humiliating, belittling, discrediting, and other forms of harm. This form of harassment among the young is characterized by the anonymity of the perpetrator, specific content and form of manifestation, as well as rapid spread and availability of violent content to a large audience, consistency, and continuity of aggression (Miladinović, Petričević, 2013).

Many local authors have spoken about the specifics of cyberbullying (Branković, 2013; Ljepava, 2011; Macanović, 2013; 2015; 2020; Macanović, Petrović, 2015; Putnik, Milošević, Bošković, 2013; Rakočević, 2019; Stanković, 2019; Stojanović, Macanović, 2022; Vrhovnik, 2013). The author Olweus (1998) states that cyberbullying possesses all the characteristics of traditional violence amongst kids. First, cyberbullying is aggressive behaviour that is expressed through negative actions, and secondly, it is always intended to hurt the victim. Third, there is always disproportionate power balance between the victim and the perpetrator, and lastly, cyber violence is characterized by repetitiveness.

It is noticeable that numerous specifics of cyberbullying relate to traditional, i.e. direct forms of violence. Cyberbullying can be present 24 hours a day, seven days a week, anywhere, at home, or in other places where a child used to feel safe. The abuser is anonymous, which increases the victim's sense of insecurity, and the audience is large and constantly increasing. Victims of violence do not necessarily have to be children, they can be adults, that is teachers and professors. Violent people sometimes cannot estimate how much damage their words can do in cyberspace, because there is no direct contact between the victim and the abuser. Messages and jokes can hurt a person without the person sending them intending to abuse anyone (Buljan-Flander, 2013).

Direct cyber violence is direct aggression against the victim, while indirect cyber violence requires the involvement of other persons, i.e. mediators in the commission of cyber violence, with and without their knowledge, but most often they are accidental accomplices who do not know and are not aware that they are a part of negative actions directed towards the victim (Popović-Ćitić, 2009).

The most common consequences of cyberbullying are low self-esteem, suicidal thoughts, frustration, depression, fear, retaliation, etc. Electronic Aggression can leave more consequences than traditional violent behaviour because it can occur at any time and anywhere in the virtual world (Batori, Ćurlin, Babić, 2020). Cyberbullying is a problem that threatens the physical and mental health of young people because it is associated with depression, anxiety, suicidal behaviour of victims, substance abuse, declining school performance, and murder in the school environment (Dragišić-Labaš, 2020). Although another person cannot be physically injured during communication in the digital world, cyberbullying has negative consequences on people's psychophysical health, the behaviour of children and adults, as well as on the emotional and social functioning of people (Kuzmanović, Lajović, Grujić, Medenica, 2016). Also, content that is humiliating and offensive to a person can be seen by a large number of people in a short period of time, which can prolong the course of abuse of the same person by persons who are not in a direct relationship with him. In addition, the same content can remain permanently online, and follow victims throughout their life. Inappropriate and offensive content can be made available to a large number of people, making the victim of violence even more helpless. If a person is verbally assaulted directly, they are unlikely to remember every word sent to them by the abuser, while in the case of cyberbullying, a person can re-read the message sent to them every day through social media. Therefore, it can be said that cyber violence brings with it traumatic consequences in the form of unpleasant feelings that can last a lifetime (Batori, Ćurlin, Babić, 2020). The results of one study state that 93% of students who have suffered

cyberbullying feel sad, depressed, anxious, and hopeless, 31% feel very upset, 19% feel hurt and 18% feel ashamed (Finelhor, 2000, see in Kuzmanović, Lajović, Grujić, Medenica, 2016: 21).

3. RESEARCH ON CYBERBULLYING

There are numerous research projects focusing on cyber violence in the world, the region, and in Bosnia and Herzegovina. In 2012, IPSOS conducted a survey on cyberbullying on a sample of 18,687 citizens in 24 countries (Italy, Spain, France, Belgium, Poland, Germany, Hungary, Russia, Sweden, The UK, China, Japan, India, Indonesia, South Korea, Turkey, Canada, USA, Brazil, Argentina, Mexico, Saudi Arabia, South Africa, and Australia). The survey showed that as many as 66% of respondents are aware of cyberbullying and that they have seen, read, or heard something about this problem. 3% of respondents said that children were regularly victims of cyber violence, 21% several times, while 6% of respondents said that children were victims once or twice. 12% of parents stated that their child was a victim of cyberbullying. The highest number of cases of electronic aggression exists in India (32%), Brazil and Saudi Arabia (19%), and 15% in the United States (Ciboci, 2014).

Paying attention to the results of a survey conducted among high school students in Kenya, the research showed that the use of social media increased violence among students by as much as 63.2% and the use of drugs under environmental pressure by 64.4%. The results also showed the respondents' claims that the use of social media significantly increased the frequency of psychological abuse, as well as cyberbullying by 45.2% and 51.7% respectively. These results indicate that the use of social media among the younger generations significantly influences changes in behaviour in the direction of stimulating illicit behaviour, and therefore it is necessary to limit or monitor risky behaviours, i.e. the use of social media for wrong purposes (Muia, 2016).

A study on youth was conducted in Bosnia and Herzegovina, which shows that 85% of citizens access the Internet every day, and more than 75% have an Internet connection in their place of residence. 95.1% of respondents said they have a Facebook profile and use it daily, 83% use Viber daily, 74.7% have an Instagram profile, and 72.9% of respondents visit Youtube daily. These social media and communication networks are most often used in Bosnia. When it comes to harassment and abuse on the Internet, 51.4% of respondents said that someone once posted information or a photo without his or her permission, 39.9%

said that an indecent comment was posted on a social network about them, and 30.6% of respondents confirmed that they were victims of threats on a social network. Every third person has experienced that someone used information about them to embarrass or tease them. 49.4% of respondents stated that the reason for harassment on the Internet was a hobby or interest, 46.9% said it was the way of dressing, 29.6% stated that the reason was religious, ethnic, or racial, and 11.1% of respondents stated that the reason was good grades in school or college, i.e. jealousy. When it comes to harassment by respondents, 22.3% stated that they once made an obscene comment about someone, 22.6% that they posted a photo or information without the permission of another person, and only 3.2% admitted that they consciously published a lie about someone (Žiga et al., 2015, see Osmić, Čustović, 2018: 584).

In Banja Luka, in 2020, research was conducted in five high schools. The research aimed to determine how much young people use social media and for what purposes. The results show that 63% of students intensively use social media during the day, 32% of students responded that they access social media every hour or two and use it for some time, and only 5% of students stated that they access social media only in the morning and evening. Most students, or 82% of students, said that they use the Internet for entertainment, then 11% of students answered that they use social media to correspond with others, to acquire new knowledge and skills was responded by only 2% of students, as well as to solve school tasks and obligations 2% of students, and 3% of students use social media to follow daily events (Macanović, Bobrek Macanović, 2021).

In 2012, research titled “The use of digital technology, risks, and prevalence of digital violence among students in Serbia” was conducted in Serbia. 17 secondary and 17 primary schools participated in the research, i.e. 3,786 students, 3,078 parents, and 1,379 teachers. The obtained results show that students use the Internet most often for correspondence. About one-fifth communicate with teachers online, and about 1% are informed about school activities through the school’s website. More than one-third of students do not use the Internet at school, more than three quarters never used the e-learning platform, and only 1% of students use it every day (Popadić, Kuzmanović, 2013).

Author of the Handbook for Children, Parents and Teachers - The Role of Schools in the Prevention and Intervention of Electronic Peer Violence Vanja Rakočević states that electronic aggression is a serious and persistent problem among children and youth. Various studies have shown that a large number of children and young people are affected by this problem, and the data of the conducted research speak about the seriousness of the problem and call for comprehensive action in Montenegro (Rakočević, 2019: 12).

Young people publish more and more information about themselves on social networks, the events they participate in, and their activities, but also information that makes them vulnerable and accessible to malicious people. A lot of information about young people can be learned from posts on their profiles; where they live, with whom they hang out, how and where they spend their free time, what interests them, where they travel, which school and which class they go to, one can even follow the daily travel routine. Young people present information about their family members, and more often about their friends without their consent and knowledge (Matijević, 2014).

The Pew Research Center published research by Mary Maden et al., 2013 on youth, social media and privacy (Maden et al., 2013) which shows that most young people post their photos on their profiles and to a lesser extent the name of the school and the city where they live, and their email address. According to the mentioned research, older minors are more inclined to present personal data than younger ones, who are more careful about publishing their photos, addresses or phone numbers. As many as 16% of young users of social networks set the settings on their profiles so that their location is automatically displayed when posting, and 18.6% state that they have experienced this inconvenience. 60% of young *Facebook* users said they keep their profiles closed to friends and believe they manage their profile in this way, but only 9% are concerned that third parties may have access to their posts. Young people have an average of 300 friends, with girls being more inclined to build wider social networks than boys, but girls are more likely to keep their profile open to friends only (70% of girls and 50% of boys make their profile available only for friends). Young people who have more than 600 friends will be less likely to accept parents as friends than young people who have fewer friends on *Facebook*.

All the above research, as well as data on the use of social networks, indicate the widespread use of the Internet among children and young people, but also the presence of cyberbullying and its consequences.

4. METHODOLOGICAL FRAMEWORK OF THE RESEARCH

4.1. The aim of the research

The research aims to determine the presence and manner of cyberbullying amongst high school students in the municipality of Modriča, as well as the con-

nection of this phenomenon with the educational and demographic characteristics of the respondents.

4.2. Research hypotheses

Main hypothesis: It is assumed that cyberbullying is present in high schools in the municipality of Modriča and that there is a statistically significant difference in the way of cyberbullying among students concerning the educational and demographic characteristics of respondents.

Special hypotheses:

H1. Various forms and methods of cyberbullying can be identified and determined among students at the Public Institution High School “Jovan Cvijić” Modriča.

H2. It is expected that there is a statistically significant difference between the forms and methods of cyberbullying that was determined among students and their success in school at the Public Institution High School Center “Jovan Cvijić” Modriča.

H3. It is assumed that there is a statistically significant difference between the forms and methods of cyberbullying that occurs in students and the place of residence of students at the Public Institution High School Center “Jovan Cvijić” Modriča.

4.3. Research variables

Within the research, variables are defined, which are integral parts of the defined research hypotheses.

Independent variables:

- School success;
- Student’s place of residence.

Dependent variables:

- Abuse through pictures and videos on the phone;
- Abuse via SMS;
- Abuse through E-mail;
- Abuse through telephone calls;
- Abuse through websites;
- Abuse through interactive games;

- Abuse by sending pornographic content;
- Attack through password theft and profile hacking.

4.4. Research methods and techniques

This research uses general and basic scientific methods, i.e. induction and deduction methods, analysis and synthesis methods, testing method, content analysis method, statistical method, comparative method and theoretical description method.

To investigate the frequency and characteristics of cyberbullying problems, the researchers used a survey method, using a survey technique, which was conducted using a questionnaire based on a questionnaire created by the research team of Goldsmith College, University of London. Surveying is a very complex method of collecting data on social reality. The examination is realized by asking clear and unambiguous questions to the respondent who answers voluntarily and consciously (Termiz, 2004). For this research, a questionnaire consisting of 21 questions was constructed. The questionnaire was used as a primary source for gathering relevant facts about cyberbullying in adolescents in high schools.

The processing of the research results was realized by applying the software package for statistical data processing SPSS 21.00 for Windows.

4.5. Population and sample research

The population from which the research sample was structured represented the total number of high school students in the municipality of Modriča. The research sample consists of 343 students of both sexes and from all four grades of several high schools (Grammar School, School of Economics and Electrical Engineering School) in the Public Institution High School Center “Jovan Cvijić” in the municipality of Modriča. The age of the respondents ranges from 15 to 18 years of age. The sample of respondents is considered representative because its characteristics resemble the basic set or population of the research.

The period of conducting the research covered the period from December 2020 to February 2021, i.e. after the end of the first semester of the school year. Therefore, the success of the first semester was taken into account for the first-grade students. The survey of students was conducted in groups, during school hours.

The research was conducted during the COVID-19 pandemic, which made it significantly more difficult to survey students, due to the need to adhere to protection measures, shortened school hours, and the absence of children from school.

5. RESEARCH RESULTS AND DISCUSSIONS

5.1. Presence of cyberbullying in high schools in the municipality of Modriča

The first special hypothesis (H1) that was set in the research was related to the identification and determination of various forms and methods of cyberbullying among high school students in the municipality of Modriča. To test this hypothesis, the data collected was analyzed on the presence of cyberbullying victims. The number of victims was also analyzed according to the forms and methods of cyberbullying.

Table 1. Presence of cyberbullying in high school students

Student victims of cyberbullying	Number of students	
Yes	136	39.7%
No	207	60.3%
Total	343	100%

Looking at the data presented in Table 1, it can be noticed that out of 343 surveyed students in high schools, 136 or 39.7% of them stated that they were victims of cyberbullying, and 207 or 60.3% of students answered that they were not victims of cyberbullying.

Based on the presented data, we can determine that a far higher number of students answered that they were not victims of violence via the Internet. However, the numbers show that cyber violence is present among the students at the Public Institution High School Center "Jovan Cvijić". Again, there is a possibility that several students answered incorrectly, that is, it is possible that some students answered out of fear that they were not victims of cyberbullying because they think that in that way they can be targeted by cyberbullies again.

5.2. Forms and ways of cyberbullying in high schools in the municipality of Modriča

Table 2 shows the relationship between the number of victims and the forms and manner of committing cyberbullying. That is, according to the data collected from students, it is stated how many students were victims of certain forms and ways of committing cyber violence.

Table 2. Presentation of the manner and form of cyberbullying concerning the number of victims

Victims of cyberbullying through different forms	SMS texts	Phone calls	Pictures	E-mail	Chat rooms	Web sites	Porno content	Online games	Hacking of profiles and theft of passwords	Total
Yes	20	20	19	8	12	11	15	10	21	136
	14.7%	14.7%	14%	5.9%	8.8%	8.1%	11%	7.4%	15.4%	100%
Total	20	20	19	8	12	11	15	10	21	136

The data shown in Table 2 indicates that of the total number of students who admitted to being victims, 20 or 14.7% were victims of cyberbullying by sending inappropriate and offensive text messages, and 20 or 14.7% of students were victims of cyberbullying through phone calls. 19 or 14% of students were victims of cyberbullying by receiving inappropriate and offensive images. 8 or 5.9% of students were harassed and abused by email, and 12 or 8.8% of students in chat rooms. 11 or 8.1% of students were abused and harassed through websites. 15 or 11% of students experienced abuse through obtaining pornographic content, and 10 or 7.4% of students through interactive games. 21 or 15.4% of students experienced an attack through profile hacking and password theft.

Analyzing the presented data, it can be seen that the most common forms and ways of cyber violence are those that manifest themselves via mobile phones, i.e. by sending harassing and malicious SMS messages, pictures and making calls. The reason for this is the fact that almost all young people in their adolescence own a smartphone and spend most of their free time using the services of the Internet and smartphones, so they are exposed and become targets of cyberbullies.

Hacking profiles and password theft are among the most common ways and forms of cyberbullying. It comes up here again that all surveyed students have a profile on one of the social networks, and that sometimes they do not protect their accounts out of ignorance, so they can easily become victims of cyberbullying. Cyber violence by sending porn content stands out as one of the more present forms of internet violence in high schools in the municipality of Modriča. One of the reasons is that in this period young people are still not mature enough to be able to judge for themselves who they should contact, i.e. they are still not able to protect themselves from paedophiles and people who refer such content to others.

5.3. The presence of forms and methods of cyberbullying in students in relation to school success

Another special hypothesis (H2) that was set in the research was whether there is a statistically significant difference between the forms and methods of cyberbullying that occurs in students at the Public Institution High School Center “Jovan Cvijić” and school success.

Table 3. Presence of forms and methods of cyberbullying in relation to the school success of high school students

Forms and methods of cyberbullying of victims	Success in schools with victim students				
	Excellent	Very Good	Good	Satisfactory	Total
SMS texts	3	8	9	0	20
	15%	40%	45%	0%	100%
Phone calls	13	6	1	0	20
	65%	30%	5%	0%	100%
Pictures	10	6	3	0	19
	52.6%	31.6%	15.8%	0%	100%
E-mail	4	3	1	0	8
	50%	37.5%	12.5%	0%	100%
Chat rooms	6	4	2	0	12
	50%	33.3%	16.7%	0%	100%
Websites	6	4	1	0	11
	54.5%	36.4%	9.1%	0%	100%
Porn content	3	7	5	0	15
	20%	46.7%	33.3%	0%	100%
Online games	2	6	1	1	10
	20%	60%	10%	10%	100%
Profile hacking and password theft	8	9	4	0	21
	38.1%	42.9%	19%	0%	100%
Total	55	53	27	1	136
	40.4%	39%	19.9%	0.7%	100%
df	24				
χ^2	36,878				
C	0,462				

Analyzing the data from Table 3, out of a total of 136 students who were victims of cyberbullying, 55 or 40.4% were students with excellent results, 53 or 39% were students with very good school results, then 27 or 19.9% are students with good re-

sults, while 1 or 0.7% are students with sufficient school success. Of the total number of students, 20 students answered that they were abused and harassed by receiving SMS messages, of which 3 or 15% are students with excellent results, 8 or 40% are students with very good results, then 9 or 45% are students with good results, and none of the students with sufficient success. 20 students answered that they were victims of cyberbullying by receiving harassing phone calls, and of that number, 13 or 65% are students with excellent results, 6 or 30% are students with very good results, and 1 or 5% are students with good results. There were no students with sufficient success. 19 students answered that they were abused and harassed by receiving disturbing and inappropriate pictures, of which 10 or 52.6% were students with excellent school results, 6 or 31.6% were students with very good results and 3 or 15.8% are students with good results. 8 students answered that they were harassed by receiving emails, i.e. 4 or 50% are students with excellent results, 3 or 37.5% are students with very good school results and 1 or 12.5% are students with good results success, while no student with sufficient school success has been a victim of cyberbullying in this way. In the chat rooms, 12 students experienced cyberbullying, i.e. 6 or 50% were students with excellent results, 4 or 33.3% were students with very good results, 2 or 16.7% were students with good results, and none the student with sufficient success was not abused in this way. 11 students experienced cyber violence through content from websites, i.e. 6 or 54.5% are students with excellent results, 4 or 36.4% are students with very good school results, and 1 or 9.1% are students with good school results success. Interestingly, no student with sufficient school achievement responded that they had been abused in this way. 15 students experienced abuse through receiving pornographic content, i.e. 3 or 20% were students of excellent school performance, 7 or 46.7% were students of very good school performance, and 5 or 33.3% were students with good school performance. 10 students answered that they were victims of cyberbullying while playing interactive games, i.e. 2 or 20% are students with excellent results, 6 or 60% are students with very good results, then 1 or 10% are students with good school results, and 1 or 10% is a student with sufficient school success. 21 students experienced an attack through password theft and profile hacking, i.e. 8 or 38.1% are students with excellent results, 9 or 42.9% are students with very good school results, 4 or 19% are students with good results, and no student with sufficient school achievement responded that he had been abused in this way.

From the data presented in Table 3, the conclusion is that there is a statistically significant difference between the form and manner of cyberbullying and school success. This fact is confirmed by the calculated chi-square. The determined $\chi^2 = 23.639$ at $df = 24$ is statistically significant at 0.05, thus confirming the fourth hypothesis.

According to the obtained data, it is concluded that students with better results, i.e. excellent and very good students are more endangered relative to students with worse, i.e. good and sufficient results.

5.4. Presence of forms and methods of cyberbullying in students in relation to the place of residence

The third special hypothesis (H3) that we set in our research was whether there is a statistically significant difference between the forms and methods of cyberbullying that occurs in students at the Public Institution High School Center “Jovan Cvijić” and place of residence.

Table 4. Presence of forms and methods of cyberbullying in students in relation to the place of residence of the student

Form and method of cyberbullying	Place of residence			
	City	Suburb	Village	Total
SMS text	11	7	2	20
	55%	35%	10%	100%
Phone calls	13	4	3	20
	65%	20%	15%	100%
Pictures	6	5	8	19
	31.6%	26.3%	42.1%	100%
E-mail	7	0	1	8
	87.5%	0%	12.5%	100%
Chat rooms	3	5	4	12
	25%	41.7%	33.3%	100%
Websites	2	7	2	11
	18.2%	63.6%	18.2%	100%
Porn content	4	5	6	15
	26.7%	33.3%	40%	100%
Online games	6	2	2	10
	60%	20%	20%	100%
Profile hacking and password theft	5	7	9	21
	23.8%	33.3%	42.9%	100%
Total	57	42	37	136
	41.9%	30.9%	27.2%	100%
df	16			
χ^2	30.503			
C	0.428			

According to the data shown in Table 4, it is concluded that out of a total of 136 students who answered that they were victims of cyberbullying, 57 or 41.9% are students living in urban areas, 42 or 30.9% are students living in the suburbs, and

37 or 27.2% are students living in the countryside. Of the total number of students, 20 students confirmed that they were victims of cyber violence by receiving SMS messages, of which 11 or 55% are students living in urban areas, 7 or 35% are students from suburban areas, and 2 or 10% are students living in the countryside. 20 students answered that they were victims of cyberbullying by receiving disturbing phone calls. That is, 13 or 65% are students from urban settlements, 4 or 20% are students from suburban settlements, and 3 or 15% are students from rural areas. 19 students confirmed that they were victims of cyber violence by receiving disturbing and inappropriate images, i.e. 6 or 31.6% are students living in urban areas, 5 or 26.3% are students living in suburban areas, while 8 or 42, 1% of students live in the countryside. Then, 8 students answered that they were abused by receiving emails, i.e. 7 or 87.5% are students from urban areas, 1 or 12.5% are students living in rural areas, while no student from suburban areas was a victim of cyber violence in this way. In the chat rooms, 12 students answered that they had experienced cyberbullying, i.e. 3 or 25% are students living in urban settlements, 5 or 41.7% are students from suburban settlements, and 4 or 33.3% are students from rural areas. 11 students experienced cyber violence through content from websites, i.e. 2 or 18.2% are students from urban settlements, 7 or 63.6% are students from suburban settlements, and 2 or 18.2% are students from rural areas. The research found that 15 students experienced abuse and harassment through pornographic content, of which 4 or 26.7% were students from urban areas, 5 or 33.3% were students living in suburban areas, and 6 or 40% were students who live in the countryside. Then, ten students answered that they were abused and harassed while playing interactive games, of which 6 or 60% were students from urban areas, then 2 or 20% were students from suburban areas, and 2 or 20% were students from rural areas. Assault through password theft and profile hacking was experienced by 21 students, i.e. 5 or 23.8% are students living in urban areas, 7 or 33.3% are students from suburban areas, and 9 or 42.9% are students who live in the countryside.

According to the data presented in the table, the researchers concluded that there is a statistically significant difference between the forms and methods of committing cyber violence, which was determined among students of the Public Institution High School Center "Jovan Cvijić" and the place of residence of students. This statement is confirmed by the determined chi-square, which in this case is $\chi^2 = 30,503$ and with $df = 16$ is statistically significant at the level of 0.05, based on which we determine that there is a statistically significant difference between the identified forms and methods of cyber violence and places student residence. Based on that, the conclusion is that this hypothesis has been confirmed.

Analyzing the presented data, the victims of aggression are more often students living in urban areas, and the smallest number of victims of cyber violence are stu-

dents living in rural areas. One possible reason is that there is a presumption that children in rural areas are less exposed to the use of the Internet and social networks, i.e. they spend more time in rural activities. Comparing the data, it is visible that abuse and harassment via text messages, phone calls, sending pictures and emails, and playing online games were reported by more students living in urban areas compared to students living in suburbs. Also, harassment and abuse by sending SMS messages, phone calls, and sending e-mails is more present in urban areas compared to rural areas. Children living in villages were more often abused and harassed by sending harassing pictures, emails, sending porn content, and hacking profiles and stealing passwords compared to children living in suburbs.

Observing the results of the research related to the conditionality of the occurrence of cyber violence and the place of residence of students, it can be concluded that the number of victims of cyber violence is the highest in the urban environment.

6. CONCLUSION

Internet violence, known worldwide as cyberbullying, is a general term for any cyberbullying communication activity that could be considered harmful to both the individual and the common well-being. This paper presents an empirical study that gives a clear perception of this problem in society. It is especially indicative that in the analysis of data related to the purpose of using the Internet and social networks, the researchers found that 100% of surveyed students have a profile at least on some form of a social network. *Facebook* (47.2%) and *Instagram* (30.9%) stood out as the two most popular social networks.

Based on the presentation of special hypotheses, the general hypothesis can be remarked. The general hypothesis that was set in the research assumed that cyberbullying is present in high schools in the municipality of Modriča and that there is a statistically significant difference in the way cyberbullying occurs among students in high schools in the municipality of Modriča in relation to educational and demographic characteristics. We can talk about the presence of cyberbullying in high schools based on the number of victims and the number of students who admitted that they once abused others on the Internet. Based on the obtained results, the researchers determined that there are students who are victims of aggression on the Internet (39.7%), but also students who have committed violence against others (28.3%). All forms of cyberbullying are present among high school students in the municipality of Modriča. Hacking of profiles and theft of passwords (15.4%) appear as the most common form and manner of cyberbullying in high schools in the municipality of Modriča. In addition, other forms and methods of cyberbullying that appear in a high percentage are sending harassing SMS messages (14.7%), making

harassing phone calls (14.7%), and sending harassing pictures (14%). The connection between the manner of cyberbullying and the educational and demographic characteristics of high school students in the municipality of Modriča was identified, i.e., we found that there is a statistically significant difference between the way cyberbullying is done and school success, as well as the place of residence of students.

Based on the data presented in this paper, it was intended to point out the fact that at any moment today anyone is in danger of becoming a target of cyberbullies, not only children and youth but also the adult population. It is apparent that children and young people are the most accessible targets and the most vulnerable part of the population in this field. Today, children and young people grow up with smartphones and social networks and these are an integral part of their daily lives, but we must be aware that these will become both an inevitable and growing companion of their growing up. That is why it is necessary to understand the real risks and problems that cyberbullying brings with it and to protect young people, but also the adult population.

REFERENCES

1. Batori, M., Ćurlin, M., Babić, D. (2020). Internet violence among adolescents. *Health Gazette*, 6 (1), p. 104 - 114.
2. Brankovic, S. (2013). Social networks and new opportunities for social research. *Culture Policy*, no. 20, year X, p. 77 - 90.
3. Buljan-Flander, G. (2013b). *Specifics of children involved in cyberbullying - implications for treatment*. Zagreb: Association of Croatian Psychotherapeutic Associations "Shades of Psychotherapy".
4. Ciboci, L. (2014). Hate groups on social networks - new forms of violence among children and youth. In: Majdak, M. et al. (ed.), *Violence on the Internet among and against children and young people* (pp. 13 - 27). Zagreb: Society for Social Policy.
5. Dimitrijević, A. (2018). Violence on Facebook among primary school students. In: Macanović, N., Petrović, J., Jovanić, G. (ed.), *No to violence - a unique social response* (pp. 195 - 202). Banja Luka: Center for Modern Knowledge.
6. Dragišić-Labaš, S. (2020). *Suicidal behaviour in adolescents and young adults: Consideration of risk factors*. Belgrade: Faculty of Philosophy.
7. Jugović, A. (2018). Behavioural problems of school-age children: Conceptual frameworks, features and implications for educational policy. In: Lazarević, E., Gutvajn, N., Malinić, D., Ševa, N. (ed.) *Improving the quality and accessibility of education in Serbia*. Belgrade: Institute for Pedagogical Research.

8. Karamazan, K. (2016). Internet addiction and electronic violence among primary school students. In: Vejmelka, L., Vuga, A., Radat, K. (ed.) *Proceedings of the 2nd Conference on Addiction Prevention: Alcoholism, Drug Addiction and Recent Addictions* (pp. 99 - 108). Zagreb: Society for Social Support.
9. Kuzmanović, D., Lajović, B., Grujić, S., Medenica, G. (2016). *Digital violence - prevention and response*. Belgrade: Ministry of Education, Science and Technological Development of the Republic of Serbia and the Pedagogical Society of Serbia.
10. Ljepava, N. (2011). *Real abuse in a virtual environment: Prevention and intervention in cases of child abuse on the Internet*. Belgrade: RODITELJ Citizens' Association.
11. Macanović, N. (2013). Peer violence as a reflection of society dysfunction. In: Šikman, M. (ed.), *Peer violence - etiology, phenomenology, ways of overcoming and comparative experiences* (pp. 131 - 141). Banja Luka: College of Internal Affairs.
12. Macanović, N. (2015). *Pedagogical current events*. Banja Luka: Center for Modern Knowledge.
13. Macanović, N. (2020). *Socially maladapted behavior of children and adolescents*. Banja Luka: Center for Modern Knowledge.
14. Macanović, N., Bobrek Macanović, K. (2021). Application of social media in the function of modern youth education. In: Macanović, N., Petrović, J., Jovanić, G. (ed.), *Improving the quality of life of children and youth* (pp. 254 - 261). Banja Luka: Center for Modern Knowledge.
15. Macanović, N., Petrović, J. (2015). *Prevention of peer violence in primary schools "Let's return friendship to the classroom"*. Banja Luka: Association of Teachers and Associates of the University of Banja Luka.
16. Mandarić, V. (2012). *New media and risky behavior of children and youth*. *Theological Review*, 82 (1), p. 131 - 149.
17. Matijević, A. (2014). Violence against and among young people on the Internet. In: Majdak, M., Vejmelka, L., Radat, K., Vuga, A. (Ed.), *Proceedings of the conference - Violence on the Internet among and against children and youth*. (pp. 39 - 51). Zagreb: Society for Social Support.
18. Miladinovic, A., Petricevic, V. (2013). *Electronic peer violence*. Banja Luka: Faculty of Security Sciences.
19. Miliša, Z. (2012). *The dark side of the screen*. Varaždin: Tiva.
20. Muia, W. (2016). Influence of social media on deviant behaviour among secondary school students in Langata, University of Nairobi.
21. Olweus, D. (1998). *Violence among children at school*. Zagreb: Školska knjiga.

22. Osmančević, L. (2016). Media in education. In: Vejmelka, L., Vuga, A., Radat, K. (ed.), *Proceedings of the 2nd Conference on Addiction Prevention: Alcoholism, Drug Addiction and Recent Addictions* (pp. 76 - 83). Zagreb: Society for Social Support.
23. Osmic, A., Custovic, E. (2018). Cyberbullying in Bosnia and Herzegovina. In: Macanović, N., Petrović, J., Jovanić, G. (ed.), *No to violence - a unique social response* (pp. 581 - 587). Banja Luka: Center for Modern Knowledge.
24. Popadić, D., Kuzmanović, D. (2013). *Use of digital technology, risks and prevalence of digital violence among students in Serbia*. Belgrade: Institute of Psychology.
25. Popović-Čitić, B. (2009). Peer violence in cyberspace. *Temida*, Vol. 12, No.3, p. 43-62.
26. Putnik, N., Milosevic, M., Boskovic, M. (2013). Electronic violence - A new form of peer violence. In: Šikman, M. (ed.), *Peer violence (etiology, phenomenology, ways of overcoming and comparative experiences)* (str. 293 - 306). Banja Luka: College of Internal Affairs.
27. Rakočević, V. (2019). *The role of school in the prevention and intervention of electronic peer violence - Handbook for children, parents and teachers*. Podgorica: NGO Children of Montenegro.
28. Stanković, D. (2019). Cyber violence on social networks among young people in the Republic of Serbia. *RKKP*, no. 2/19, p. 9 - 23.
29. Stojanović, R., Macanović, N. (2022). *Cyberbullying*. Banja Luka: Center for Modern Knowledge.
30. Termiz, J. (2004). *Methodology of social sciences*. Sarajevo: University of Sarajevo.

Online sources:

1. Maden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., Beaton, M. (2013). *Teens, Social Media and Privacy*, Pew Research Center. On the website: <http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy>. Read: 09.04.2022.
2. Vrhovnik, A. (2013). *Electronic violence among children and young people*. Zagreb: Faculty of Philosophy. On the website: www.researchgate.net. Read: 18 December 2021.

Prof. dr Nebojša Macanović
Vanredni profesor, Fakultet političkih nauka, Univerzitet u Banja Luci,
Bosna i Hercegovina

Ružica Stojanović
Dnevni centar za decu sa specijalnim potrebama „Sunce Obervalisa“

CYBERBULLYING KAO OBLIK VRŠNJAČKOG NASILJA U ŠKOLAMA

Nasilje putem interneta, u svijetu poznato kao cyberbullying, opšti je pojam za svaku komunikacijsku aktivnost sajber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opšte dobro. Sve veći broj djece i mladih je izloženo vršnjačkom nasilju putem interneta, ali i pored toga zabrinjava činjenica da i dalje ono nije prepoznato kao ozbiljan problem u društvu. Jedan od razloga zbog kojih ovaj trend nije zabrinjavajući leži u činjenici da se on događa u virtualnom svijetu, te da nije prisutan u “stvarnom djetetovom okruženju. Cilj ovog rada jeste prikaz empirijskog istraživanja kojim smo željeli da utvrdimo prisutnost i način vršenja sajberbulinga kod učenika u srednjim školama u opštini Modriča, kao i povezanost ove pojave sa obrazovnim i demografskim karakteristikama ispitanika. U našem istraživanju bazirali smo se na učenike i školu kao mjesto gdje se često identifikuju ovi problemi kod mladih. Rezultati istraživanja ukazali su na karakteristike sajberbulinga, ali i na uzroke i posljedice ove pojave.

KLJUČNE RIJEČI: nasilje / cyberbullying / internet / društvene mreže / škola

CYBERBULLYING AND CYBER VICTIMISATION: A LITERATURE REVIEW OF ASSESSMENT INSTRUMENTS

Milena MILIĆEVIĆ, PhD¹

The knowledge regarding cyberbullying and its consequences has increased during the past two decades. A more detailed insight into the characteristics of cyberbullying and cyber victimisation requires a significant diversity of measures. However, no agreement on the best measurement method has been reached. The present literature review aimed to identify and present the instruments and measures constructed and utilised to assess cyberbullying and/or cyber victimisation. A systematic search identified 2031 publications. The selection process resulted in 11 assessment instruments, which were analysed. According to the findings, the starting point in the construction or adaptation of assessment instruments specific to our context should be a consistent, enhanced and standardised definition of cyberbullying comparable to the ones used worldwide, followed by the precise criteria for the representativeness of the target population and carefully considered both socio-cultural factors and the time frame. Finally, it is necessary to conduct comprehensive statistical analyzes in order to develop and verify the psychometric properties of the cyberbullying assessment tool that would be adequate for the assessment of this phenomenon in Serbia.

KEY WORDS: cyberbullying / measurement / assessment / cyber harassment

¹ Senior Research Fellow, Institute of Criminological and Sociological Research in Belgrade, mileninaadresa@gmail.com

1. INTRODUCTION

In the past two decades, there has been a noticeable expansion of the research interest in cyberbullying phenomenon (Antoniadou & Kokkinos, 2015; Baltezarovic et al., 2016). Cyberbullying is typically defined as a form of bullying others by using electronic communication technologies or information and communications technologies (ICTs) to carry out psychological peer harassment (Kowalski et al., 2014). The experience of cyberbullying has been linked to “an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend himself or herself” (Smith et al., 2008, p. 376).

Research on cyberbullying is no longer at an early stage. To gain a context-appropriate understanding of the cyberbullying phenomenon, its diverse features should be captured. Therefore, the research focus has extended and now involves different context and disparate populations and various online communication media and ICTs. However, a measurement problem is still prevalent in recent literature (Chun et al., 2020; Kowalski et al., 2014). Nature of items capturing the full conceptual domain of cyberbullying phenomenon and their pooling method, differences in sample characteristics (e.g., age, gender, socio-cultural context), bullying or cyberbullying definition provision, theoretical basis or background that provides a comprehensive framework for different person and situational factors included, are some of the challenges listed (Chun et al., 2020; Kowalski et al., 2014). Even though the knowledge base regarding the nature of the cyberbullying problem has increased, no agreement on the best method of measuring these experiences has been reached.

Cyberbullying continues to be a serious issue, associated with many psychosocial and physical problems, including diverse mental health outcomes and various problems of a psychosomatic nature (Annerback et al., 2014; Bonanno & Hymel, 2013; Chang et al., 2013; Edwards et al., 2016; Fridh et al., 2015; Kowalski & Limber, 2013; Mitchell et al., 2007; Olenik-Shemesh et al., 2012; Schneider et al., 2012; Shapka & Maghsoudi, 2017; Sourander et al., 2010). Given the adverse outcomes of cyberbullying and/or cyber victimisation, the research question arises about the possibilities of assessing the characteristics, aspects and components of this phenomenon in society. This paper aims to identify and present the instruments and measures utilised to assess cyberbullying and/or cyber victimisation by conducting an extensive literature review and synthesising the findings in this field.

2. METHODS

An extensive literature search was performed to identify relevant studies conducted to develop, validate and/or investigate the psychometric properties of different measures of cyberbullying. The comprehensive search was performed by using Google Scholar – Advanced Scholar Search. Scholarly manuscripts published in English since January 1, 2000, were included. The following keywords were used with multiple combinations: “measure”, “survey”, “inventory”, “questionnaire”, “scale”, “test” (with all of the words) combined with “cyberbullying”, “cyber bullying”, “cyber victimisation” and “cyber victimisation” (with the exact phrase). Next, studies citing selected measures were further explored at the level of titles and abstracts. The following studies were considered eligible: studies that developed the cyberbullying scale or used a scale in modified or revised version; published in English; focused on cyberbullying perpetration, victimisation, or both; studies including a sample of children, adolescents, or adults; and original, peer-reviewed articles or doctoral dissertations. The literature search resulted in a total of 1353 citations, and an additional 678 were screened at the title and abstract level. Using the above criteria, and after excluding the duplicates, 11 different measures utilised to assess cyberbullying and/or cyber victimisation are included in this literature review. The search was completed in April 2022.

3. REVIEW OF MEASURES UTILISED TO ASSESS CYBERBULLYING AND/OR CYBER VICTIMISATION

3.1. Cyberbullying Experiences Survey

The Cyberbullying Experiences Survey (CES) is a reliable and valid multifactor survey developed to assess cyberbullying victimisation and perpetration in the emerging adult population (Doane et al., 2013). The main strength of this survey is that it covers different forms of cyberbullying. According to the authors, the frequency and variability of cyberbullying among a college student population needed more closely examination (Doane et al., 2013).

The CES consists of a 21-item victimisation subscale and a 20-item perpetration subscale. Each subscale covers four factors: unwanted contact, malice, deception, and public humiliation. These four factors were previously identified as the most frequent types of incidents reported by cyber victims (Doane et al., 2009, as cited in (Doane et al., 2013)). All items are given in a form of questions and

rated on a 6-point Likert-type scale in terms of frequency of experience ranging from *Never* to *Every day/Almost every day*. Instead of providing an operational definition of cyberbullying, questions are focused on cyberbullying behaviours. A total of 29 different cyberbullying behaviours are included, with 12 behaviours overlapping between the two subscales and 17 behaviours not overlapping: unwanted contact (nine items), malice (six items), deception (three items), and public humiliation (11 items). Two examples of survey items include, “Has someone changed a picture of you in a negative way and posted it electronically?” and “Have you lied about yourself to someone electronically?”

The CES was confirmed as a useful tool for understanding demographic differences and predictors of cyberbullying perpetration among college students (Bauman & Baldasare, 2015; Doane et al., 2013). Moreover, the CES was used for the evaluation of the effectiveness of cyberbullying prevention and intervention programs (Doane et al., 2016, 2020) and the role of optimism as a protective factor against the negative impact of cyberbullying at work (Snyman & Loh, 2015). Later results have demonstrated its utility in both explorative and applied research, in different socio-cultural settings (Bauman & Baldasare, 2015; Ndiege & Kanyi, 2018; Somma et al., 2022), for studying cross-cultural differences in cyberbullying perpetration frequency and process (Barlett, Seyfert, et al., 2021), but also during the COVID-19 era (Barlett, Simmers, et al., 2021; Doane et al., 2020).

3.2. Workplace Cyberbullying Measure

The first workplace-specific cyberbullying instrument is the Workplace Cyberbullying Measure (WCM), designed and developed to assess cyberbullying across a broad spectrum of ICTs and diverse working populations (Farley et al., 2016). The tool is composed of a total of 17 items capturing employees’ exposure to cyberbullying through technology in relation to their work context over the previous six months: 10 items on work-related cyberbullying and seven items on person-related cyberbullying. The response options are *Never*, *Now and then*, *At least monthly*, *At least weekly* and *Daily*, with the latter two options being merged after a statistical analysis. According to the authors, the WCM captures exposure to negative work-related acts experienced through ICTs, including one item that evaluates the power disparity criterion between perpetrator(s) and victim and allows self-labelling as victims. Respondents answer this one question after completing the cyberbullying items and after being presented with the refined workplace cyberbullying definition. The response options are *No*, *Yes, now and then*, *Yes, monthly*, *Yes, weekly* and *Yes, almost daily*. Two examples of measure items include, “Received messages that contain abusive language aimed at you” and “Received aggressive-

ly worded messages (e.g. using all capital letters, bold font or multiple exclamation marks)”.

The results confirmed that respondents experiencing more behaviours more frequently tended to perceive themselves as being less capable of defending themselves (Farley et al., 2016). The main advantage of the WCM is its validity as a single-factor model and as a two-factor model comprising work-related cyberbullying and person-related cyberbullying. Furthermore, practical implications include using this measure as a list of indicators that employees find unacceptable in their work settings (Farley et al., 2016).

Overall usability of the WCM was confirmed in different socio-cultural and working contexts, including the Covid-19 pandemic (K. Y. Kim & Choi, 2021; Nikolić et al., 2017; Park & Choi, 2019; Z. Zhang et al., 2021). Recently, the WCM was used to investigate the roles of psychological distress between workplace cyberbullying and creativity (Kalyar et al., 2021) and the daily influence of workplace cyberbullying on interpersonal deviance (Z. Zhang et al., 2021). Moreover, it was used to determine individual and organizational factors influencing workplace cyberbullying (Y. Kim & Choi, 2021) and the antecedents of workplace cyberbullying, such as the perpetrator traits and unique occurrence environment in the context of workplace cyberbullying (S. Zhang et al., 2022).

3.3 Inventory of Cyberbullying Acts at Work

The Inventory of Cyberbullying Acts at Work (ICA-W) is a reliable and valid tool for a quick and easy evaluation of cyberbullying occurrence in the workplace (Vranjes, Baillien, et al., 2018a). This 10-item psychometrically sound and compact measurement instrument has three-factor structure – work-related acts, person-related acts and intrusion. The ICA-W is both general and specific instrument, which is its main strength. More precisely, it can be used to determine the occurrence of cyberbullying behaviour at work or to explore different types of cyberbullying behaviours (work related, person related, intrusive). Similar to the WCM, the ICA-W assesses the cyberbullying phenomenon in the work environment. However, the ICA-W has fewer items (10 vs. 17) and covers more than a single-factor structure. Overall, there are four work related items (e.g. “Your emails are forwarded to third parties in order to harm you”), three person related items (e.g. “Constant remarks are being made about you and your private life by means of ICTs”), and three intrusive items (e.g. “Somebody takes over your identity”). All items were answered on a 5-point Likert scale with the following options: *Never*, *One time*, *Monthly*, *Weekly*, and *Daily*.

The ICA-W was used as a measure of workplace cyberbullying in different socio-cultural and working settings (Anwar et al., 2020), but also for studying cross-sectional differences between patterns of cyber victimisation and emotion regulation in subgroups of individuals based on their cyberbullying victimisation experience (Vranjes, Erreygers, et al., 2018). As recently presented, the ICA-W contributed in testing the role of stressor related emotions on exposure cyberbullying at work, further confirming its utility (Vranjes, Baillien, et al., 2018b).

3.4. Positive Attitudes toward Cyberbullying Measure

The Positive Attitudes toward Cyberbullying Measure (Barlett et al., 2016) is a self-report assessment that assesses the degree to which a person endorses positive cyberbullying attitudes. It consists of nine items and two distinct factors: Harmful Cyberbullying Attitudes (HCA; five items) and General Cyberbullying Characteristics (GCC; four items). This measure is described as brief and easy-to-administer, face valid, concurrently valid, predictively valid, with good internal consistency (Barlett et al., 2016). Moreover, its items are general and are not limited to any specific website, device, or environment. Items are given in a form of statement and responders indicate their level of agreement on a 5-point rating scale (ranging from *Strongly disagree* to *Strongly agree*). All items were summed and higher scores indicate higher pro-cyberbullying attitudes. Two examples of measure items include, “Teasing or making fun of others with harmful comments online is fun to me” and “Sending mean electronic messages to others is less harmful than face-to face communication”.

Recent results confirmed the utility of the Positive Attitudes toward Cyberbullying Measure in different cultural settings (Barlett, Seyfert, et al., 2021; Cavalcanti et al., 2021; Kumar & Sadeeq, 2020; H. Zhang et al., 2020) and longitudinal research as it was applied to analyse the longitudinal relationship between early social media use and later cyberbullying perpetration via positive cyberbullying attitudes (Barlett et al., 2018). Furthermore, this scale was used to evaluate the implementation of a theory-based video intervention program, which was designed to challenge college students’ anonymity perceptions to reduce subsequent cyberbullying (Barlett et al., 2020). Also, this measure was used to investigate a mediating model of relationship between childhood psychological abuse and cyberbullying perpetration attitudes (H. Zhang et al., 2020).

3.5. Cyberbullying Inventory for College Students

One of the most used measures to assess cyberbullying is the Cyberbullying Inventory for College Students (CICS) (Francisco et al., 2015; Jenaro et al.,

2018). The CICS evaluates the type and degree of involvement in cyberbullying or, more precisely, how university students perceive their involvement in acts of cyberbullying. The final version of the CICS consists of 42 close-ended questions organized into four scales: for victims (nine items, e.g. “They spread rumors about my life”), for aggressors (eight items, e.g. “I made fun of someone”), for observers of the victim (nine items, e.g. “Someone made fun of them”), and for observers of the aggressor (nine items, e.g. “They made fun of someone”). The response options are *Never*, *Sometimes* and *Many times*. A special characteristic of this inventory is that it collects information about the technologies used in victimisation/aggression acts (e.g. computer, cell phone; Facebook, Messenger, Myspace, YouTube, SMS). Coping strategies used by victims (e.g. “I deleted my Facebook page”) and motives aggressors mentioned for cyberbullying others (e.g. “Because I don’t like the person’s attitudes”) are noted, as well (Francisco et al., 2015). The CICS was later used to investigate whether student bystander interventions can affect the relationship between being a bystander of a cyberbullying incident and being the victim or the aggressor (Ferreira et al., 2016). Another study that included the CICS as a measure to assess cyberbullying explored cultural issues influencing students’ involvement in cyberbullying situations (Souza et al., 2018).

3.6. Cyberbullying Inventory for University Students revised

The revised version of the Cyberbullying Inventory (CBI) for University Students (Topcu & Erdur-Baker, 2018) has two sections that measure cyberbullying perpetration and cyberbullying victimisation (Tanrikulu & Erdur-Baker, 2021). Respondents are asked to report the frequency of listed behaviours, with the answer for the cyberbullying perpetration items given as “I did”, while the answer for cyberbullying victimisation are given as “It happened to me”. The frequency of their cyberbullying experiences as a cyber bully or a cyber victim in the last six months was rated on a 4-point Likert scale in each section: *Never*, *Once*, *Twice-three times*, and *More than three times*, with higher scores indicating a higher frequency of cyberbullying perpetration or cyber victimisation. Two examples of measure items include, “Spreading gossips and rumours online” and “Blocking someone’s access to an online account by stealing their password”. Additionally, several participants’ cyberbullying involvement categories can be created, including categories of cyberbullies, cyber victims, cyber bully-victims and non-involved (Tanrikulu & Erdur-Baker, 2021). The CBI for University Students was recently used as the criterion validity of the new Online Trolling Scale (Hamarta et al., 2021).

3.7. Cyberbullying Scale

A different approach was noted in a study conducted by Walker, Sockman, and Koehn (Walker et al., 2011). The previous versions of their 27-item Cyberbullying Scale can be found in work by (Li, 2006) and (Spitzberg & Hoobler, 2002). This scale is focused on 13 different situations received or experienced in an electronic form of communication. Example situations include the following: exaggerated messages of affection, excessively explicit messages, threatening written messages, pictures or images, sabotaging' private or work/school reputation, pornographic/obscene images or message, etc. Additionally, frequency of experiencing cyberbullying is recorded (response options: *Less than 4 times*, *4 to 10 times*, and *More than 10 times*), as well as technologies used to cyberbully (i.e., email, text or video message via cell phone, social media like Facebook or Twitter, instant messaging). Lastly, the sources of the undesirable communication is indicated, e.g. classmate, former classmate, former boyfriend/girlfriend, someone dated once or twice, roommate, family member, and do not know the person, etc. Since the scale distinguishes between the ICTs used, later application was noted in a study on the impact of risky social network site practices and individual differences in personality on the likelihood of cyberbullying victimisation among young adult Facebook users (Peluchette et al., 2015).

3.8. Cyberbullying Scale updated

The Cyberbullying Scale (CBS), developed by Stewart et al. (Stewart et al., 2014), is a broad self-report measure of cyberbullying victimisation designed to overcome limitations of the previously used scales. According to the authors, the CBS advances the field by providing greater operationalization and including a more diverse base of electronic mediums or ICTs used (Stewart et al., 2014). As a screening tool, the CBS can be used to identify students aged 11 to 18 who are being cyberbullied. On the other hand, as an outcome measure, it can be utilised for determining different cyberbullying intervention efforts.

Generally, the CBS has a single-factor structure. It consists of 14 items on frequency of experiencing different forms of cyber victimisation rated on a 5-point Likert-type scale ranging from *Never* to *All the time*. Two examples of measure items include, "How often do you get text or online messages that make you afraid for your safety?" and "How often do you get in online fights?" All items were summed and higher scores indicate more frequent experiences of being a victim of cyberbullying (Stewart et al., 2014). The final version also includes two general questions about electronic mediums through which the responders were bullied

and which they used to bully others. Overall utility of the CBS was confirmed in different cultural settings (Saman et al., 2021).

3.9. Cyberbullying Test

The Cyberbullying Test is a three-factors screening instrument design to measure cyber victimisation, cyber aggression, and cyber observation (Garaigordobil, 2017). It includes 15 behavioural categories. The focus is on three types of behaviours: respondent's own experiences of cyber victimisation, their own cyber aggressive behaviours, and the cyberbullying behaviours they observe in others, regardless of the means used. The frequency with which these behaviours were suffered, performed, or observed during the past year is recorded on a 4-point scale ranging from *Never* to *Always*. The main advantage of the Cyberbullying Test is its triangular perspective, as it rates the level of cyber victimisation, cyber aggression, and cyber observation. The Cyberbullying Test was used to explore prevalence of cyberbullying in gifted students, its prevalence and relationship with other psychological variables (González-Cabrera et al., 2019). Recently, its reliability was confirmed when the cyberbullying experience and coping manners of adolescents in urban Vietnam were explored, including the associations between cyberbullying and mental health issues (Ngo et al., 2021). The research results also confirmed that the Cyberbullying Test could be used to analyse differences in sexual orientation in relation to the position of victims or aggressors of bullying/cyberbullying, and compare the mental health of adolescent heterosexual and non-heterosexual victims, aggressors, cyber victims, and cyber aggressors (Garaigordobil & Larrain, 2020).

3.10. Electronic Bullying Questionnaire

The Electronic Bullying Questionnaire (EBQ) was first presented as a 23-item self-report measure by Kowalski and Limber (Kowalski & Limber, 2007), and later revised by Moore, Huebner and Hills (Moore et al., 2012), to evaluate cyberbullying among middle school students. The EBQ consists of cyberbullying perpetration and cyberbullying victimisation scales, each scored separately as a mean, with higher scores reflecting higher frequencies of cyberbullying (perpetration or victimisation). The revised EBQ has nine core questions that assess bullying (four items), victimisation (four items), and fear of being bullied (one item), excluding questions about the medium used (Moore et al., 2012). Prevalence questions were answered using a 5-point response format ranging from *It hasn't happened in the past couple of months* to *Several times a week*. Two examples of items include, "Has

anyone used your computer username or screen-name to spread rumours or lies about another person?” and “Have you used someone else’s computer username or screen-name to spread rumours or lies about another person?” In a recent study, the EBQ was used to examine the longitudinal associations between neuroticism and cyberbullying (perpetration and victimisation) among Chinese early adolescents (D. Zhang et al., 2020). Earlier, the EBQ was used to determine the differential mediational roles of perceived peer relationship stress in the association between cyberbullying and cyber victimisation and mental health among early adolescents in both cross-sectional data and longitudinal data (Tian et al., 2018).

3.11. Internet Experiences Questionnaire

The 47-item Internet Experiences Questionnaire (IEQ) is one of the earliest measures specifically designed to assess cyberbullying, with separate subsections focusing on perpetrators of cyberbullying, traditional bullying experiences, cyberbully victimisation separated by different forms of cyberbullying (text messaging, Internet, picture/video messaging), general cyberbullying experiences, and impact and coping methods (Schenk & Fremouw, 2012). The main challenge in applying this measure is a variety of different types of questions asked. The largest group are open-ended questions, followed by the multiple-choice and yes/no questions. Two examples of items include, “If you were a victim of cyberbullying, how did you get the harassment to stop?” and “If you have been cyberbullied in any way, what sorts of comments/ remarks were made? Please check all that apply: appearance, race, sexual orientation, etc.” The IEQ was used in a study of the impact of social relationships on bullies, victims, bully/victims, and uninvolved participants (Keelan et al., 2014), to comprehensively describe the characteristics of college cyberbullies (Schenk et al., 2013) and in a study on the psychological experience of cyberbullying among transgender adults (Macpherson, 2022).

4. CONCLUDING REMARKS

The present literature review aimed to identify and present the instruments or measures constructed and used to assess cyberbullying and/or cyber victimisation. A total of 11 assessment instruments were analysed. Aiming to characterise the phenomenon of cyberbullying accurately, many researchers opted for different approaches. A more detailed insight into the characteristics of cyberbullying and cyber victimisation requires a significant diversity of measures. At the same time, significant diversity of measures makes comparing the findings among studies difficult.

First, it should be noted that the authors conceptualised cyberbullying by using various definitional criteria. For example, the WCM relies on the same definitional criteria as traditional bullying (D'Souza et al., 2017), whereas the CBI does not provide a definition of cyberbullying (Tanrikulu & Erdur-Baker, 2021). Other authors relied solely on characteristics that differentiated traditional from electronic bullying (Moore et al., 2012).

Second, the medium used to channel an act was considered outdated or irrelevant for research purposes in a number of studies. Therefore, instruments should be considered concerning whether they assess cyber-related behaviour regardless of the medium or ICTs used. Namely, the CES contains a number of cyber-specific items without referencing the medium used (Doane et al., 2013). A similar strategy was used for the Positive Attitudes toward Cyberbullying Measure (Barlett et al., 2016) and the EBQ (Moore et al., 2012). The WCM considers various ICTs that individuals use in their work rather than through a specific medium (Farley et al., 2016). On the other hand, the CICS asks about the digital media used (Francisco et al., 2015), as the Cyberbullying Scale (Walker et al., 2011) and the CBS (Stewart et al., 2014).

Next, some instruments are context-specific or designed for a specific population. Most of the measures are focused on college students. For example, the CES was developed to assess cyber-bullying among college students (Doane et al., 2013), while the WCM has addressed work-related cyber harassment (Farley et al., 2016). Concerning the context-specificity, some measures that assess the cyber-bullying phenomenon can be used as complementary since they allow different types of negative online acts to be differentiated. Examples include the WCM (Farley et al., 2016) and the ICA-W (Vranjes, Baillien, et al., 2018a).

Regardless of the complexity of cyberbullying, some instruments allow different forms of analysis. The WCM combines behavioural items that evaluate exposure to bullying behaviour with a self-labelling definition question (Farley et al., 2016). The CICS is, on the other hand, a more comprehensive instrument as it combines perception of involvement in cyberbullying and information about the digital media used with questions inquiring about the coping strategies used by victims and bystanders about the emotions involved and the motives of the aggressor (Francisco et al., 2015). The IEQ offers a variety of types of questions allowing more comprehensive insight into different forms of cyberbullying experiences (Schenk & Fremouw, 2012).

When it comes to the time frame used to assess cyberbullying and cyber victimisation, there are some inconsistent across the presented measures. Even in those measures with a specific time frame, the authors used different time periods. For example, the previous year was covered in the CES (Doane et al., 2013)

and the Cyberbullying Test (Garaigordobil, 2017), whereas the ICA-W (Vranjes, Baillien, et al., 2018a) was focused on the previous six months. In contrast, some measures did not provide a specific time period, including the CBS (Stewart et al., 2014) and the EBQ (Moore et al., 2012) that cover the past few months and the past couple of months, respectively. Consequently, data collected using different instruments may lead to different findings on the prevalence rates of this phenomenon, further complicating interpretation and comparison of the results in the international context.

The findings of this literature review also revealed that most of the cyberbullying instruments are multifactorial or consist of several subscales. In other words, some measures utilised to assess cyberbullying are unifactorial, whereas others explore various factors. The CBS (Stewart et al., 2014) is unifactorial, whereas the WCM is both a single- and a two-factor model (Farley et al., 2016). Among the multifactorial instruments are the Positive Attitudes toward Cyberbullying Measure (Barlett et al., 2016), CES (Doane et al., 2013), ICA-W (Vranjes, Baillien, et al., 2018a), CICS (Francisco et al., 2015), CBI (Tanrikulu & Erdur-Baker, 2021), EBQ (Moore et al., 2012) and the Cyberbullying Test (Garaigordobil, 2017).

This literature review has some limitations to be considered. First, the study only included original, empirical peer-reviewed articles and doctoral dissertations, and hence, other types of manuscripts (e.g., unpublished dissertations, systematic reviews, meta-analytic studies, or government reports) were excluded. Second, the cyberbullying measurement studies published in languages other than English were also excluded, thus reducing the variance in the socio-cultural context. In addition, a quality assessment process was not conducted and studies were characterised only based on their design. These omissions may lead to selection bias in this literature review. Further studies could gather additional evidence from excluded sources.

Despite these limitations, the information obtained in the present literature review could be used to initiate the construction or adaptation of assessment instruments specific to our context. The starting point should be a consistent, enhanced and standardised definition of cyberbullying comparable to the ones used worldwide, further underlining the prominent implications for measuring cyberbullying behaviours. Clear criteria for the representativeness of the target population sample are required. Next, the socio-cultural factors need to be carefully considered to gain a context-appropriate understanding of the cyberbullying or cyber victimisation phenomenon. As stated previously, the importance of the time frame should not be overlooked. Finally, to ensure construct validity, reliability, and factor stability, comprehensive statistical analyses should be carefully conducted, thus resulting in verified psychometric properties of cyberbullying measurements.

REFERENCES

1. Annerback, E. M., Sahlqvist, L., & Wingren, G. (2014). A cross-sectional study of victimisation of bullying among schoolchildren in Sweden: Background factors and self-reported health complaints. *Scandinavian Journal of Public Health*, *42*(3), 270–277. <https://doi.org/10.1177/1403494813514142>
2. Antoniadou, N., & Kokkinos, C. M. (2015). Cyber and school bullying: Same or different phenomena? *Aggression and Violent Behavior*, *25*, 363–372. <https://doi.org/10.1016/j.avb.2015.09.013>
3. Anwar, A., Kee, D. M. H., & Ahmed, A. (2020). Workplace Cyberbullying and Interpersonal Deviance: Understanding the Mediating Effect of Silence and Emotional Exhaustion. *Cyberpsychology, Behavior, and Social Networking*, *23*(5), 290–296. <https://doi.org/10.1089/cyber.2019.0407>
4. Baltezarevic, V., Baltezarevic, R., & Baltezarevic, B. (2016). The prevalence of victimization and the internet abuse in student population. *Temida*, *19*(3–4), 373–387. <https://doi.org/10.2298/TEM1604373B>
5. Barlett, C. P., Gentile, D. A., Chng, G., Li, D., & Chamberlin, K. (2018). Social Media Use and Cyberbullying Perpetration: A Longitudinal Analysis. *Violence and Gender*, *5*(3), 191–197. <https://doi.org/10.1089/vio.2017.0047>
6. Barlett, C. P., Heath, J. B., Madison, C. S., DeWitt, C. C., & Kirkpatrick, S. M. (2020). You're not anonymous online: The development and validation of a new cyberbullying intervention curriculum. *Psychology of Popular Media*, *9*(2), 135–144. <https://doi.org/10.1037/ppm0000226>
7. Barlett, C. P., Helmstetter, K., & Gentile, D. A. (2016). The development of a new cyberbullying attitude measure. *Computers in Human Behavior*, *64*, 906–913. <https://doi.org/10.1016/j.chb.2016.08.013>
8. Barlett, C. P., Seyfert, L. W., Simmers, M. M., Hsueh Hua Chen, V., Cavalcanti, J. G., Krahe, B., Suzuki, K., Warburton, W. A., Wong, R. Y. M., Pimentel, C. E., & Skowronski, M. (2021). Cross-cultural similarities and differences in the theoretical predictors of cyberbullying perpetration: Results from a seven-country study. *Aggressive Behavior*, *47*(1), 111–119. <https://doi.org/10.1002/ab.21923>
9. Barlett, C. P., Simmers, M. M., Roth, B., & Gentile, D. (2021). Comparing cyberbullying prevalence and process before and during the COVID-19 pandemic. *The Journal of Social Psychology*, *161*(4), 408–418. <https://doi.org/10.1080/00224545.2021.1918619>
10. Bauman, S., & Baldasare, A. (2015). Cyber Aggression Among College Students: Demographic Differences, Predictors of Distress, and the Role of the

- University. *Journal of College Student Development*, 56(4), 317–330. <https://doi.org/10.1353/csd.2015.0039>
11. Bonanno, R. A., & Hymel, S. (2013). Cyber Bullying and Internalizing Difficulties: Above and Beyond the Impact of Traditional Forms of Bullying. *Journal of Youth and Adolescence*, 42(5), 685–697. <https://doi.org/10.1007/s10964-013-9937-1>
 12. Cavalcanti, J. G., de Lima Pinto, A. V., Pimentel, C. E., & de Melo, L. M. F. (2021). Psychometric Parameters of the Cyberbullying Attitude Scale in Brazil. *Current Psychology*, 40(8), 3897–3907. <https://doi.org/10.1007/s12144-019-00326-6>
 13. Chang, F. C., Lee, C. M., Chiu, C. H., Hsi, W. Y., Huang, T. F., & Pan, Y. C. (2013). Relationships Among Cyberbullying, School Bullying, and Mental Health in Taiwanese Adolescents. *Journal of School Health*, 83(6), 454–462. <https://doi.org/10.1111/josh.12050>
 14. Chun, J. S., Lee, J., Kim, J., & Lee, S. (2020). An international systematic review of cyberbullying measurements. *Computers in Human Behavior*, 113(June), 106485. <https://doi.org/10.1016/j.chb.2020.106485>
 15. D'Souza, N., Forsyth, D., Tappin, D., & Catley, B. (2017). Engaging industry specialists on the issue of workplace cyberbullying—a New Zealand study. *Journal of Health Safety and Environment*, 33(2), 105–124.
 16. Doane, A. N., Ehlke, S., & Kelley, M. L. (2020). Bystanders Against Cyberbullying: a Video Program for College Students. *International Journal of Bullying Prevention*, 2(1), 41–52. <https://doi.org/10.1007/s42380-019-00051-5>
 17. Doane, A. N., Kelley, M. L., Chiang, E. S., & Padilla, M. A. (2013). Development of the Cyberbullying Experiences Survey. *Emerging Adulthood*, 1(3), 207–218. <https://doi.org/10.1177/2167696813479584>
 18. Doane, A. N., Kelley, M. L., & Pearson, M. R. (2016). Reducing cyberbullying: A theory of reasoned action-based video prevention program for college students. *Aggressive Behavior*, 42(2), 136–146. <https://doi.org/10.1002/ab.21610>
 19. Edwards, L., Kontostathis, A. E., & Fisher, C. (2016). Cyberbullying, Race/Ethnicity and Mental Health Outcomes: A Review of the Literature. *Media and Communication*, 4(3), 71. <https://doi.org/10.17645/mac.v4i3.525>
 20. Farley, S., Coyne, I., Axtell, C., & Sprigg, C. (2016). Design, development and validation of a workplace cyberbullying measure, the WCM. *Work and Stress*, 30(4), 293–317. <https://doi.org/10.1080/02678373.2016.1255998>
 21. Ferreira, P. C., Simão, A. M. V., Ferreira, A., Souza, S., & Francisco, S. (2016). Student bystander behavior and cultural issues in cyberbullying: When ac-

- tions speak louder than words. *Computers in Human Behavior*, 60, 301–311. <https://doi.org/10.1016/j.chb.2016.02.059>
22. Francisco, S. M., Veiga Simão, A. M., Ferreira, P. C., & Martins, M. J. D. D. (2015). Cyberbullying: The hidden side of college students. *Computers in Human Behavior*, 43, 167–182. <https://doi.org/10.1016/j.chb.2014.10.045>
 23. 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*, 15(1), 1–12. <https://doi.org/10.1186/s12889-015-2239-7>
 24. Garaigordobil, M. (2017). Psychometric Properties of the Cyberbullying Test, a Screening Instrument to Measure Cybervictimization, Cyberaggression, and Cyberobservation. *Journal of Interpersonal Violence*, 32(23), 3556–3576. <https://doi.org/10.1177/0886260515600165>
 25. Garaigordobil, M., & Larrain, E. (2020). Bullying and cyberbullying in LGBT adolescents: Prevalence and effects on mental health. *Comunicar*, 28(62), 79–90. <https://doi.org/10.3916/C62-2020-07>
 26. González-Cabrera, Tourón, Machimbarrena, Gutiérrez-Ortega, Álvarez-Bardón, & Garaigordobil. (2019). Cyberbullying in Gifted Students: Prevalence and Psychological Well-Being in a Spanish Sample. *International Journal of Environmental Research and Public Health*, 16(12), 2173. <https://doi.org/10.3390/ijerph16122173>
 27. Hamarta, E., Akat, M., & Deniz, M. (2021). Development of Online Trolling Scale: Validity and Reliability Study. *Türk Psikolojik Danışma ve Rehberlik Dergisi*, 11(63), 457–470. <https://doi.org/10.17066/tpdrd.1050742>
 28. Jenaro, C., Flores, N., & Frías, C. P. (2018). Systematic review of empirical studies on cyberbullying in adults: What we know and what we should investigate. *Aggression and Violent Behavior*, 38, 113–122. <https://doi.org/10.1016/j.avb.2017.12.003>
 29. Kalyar, M. N., Saeed, M., Usta, A., & Shafique, I. (2021). Workplace cyberbullying and creativity: examining the roles of psychological distress and psychological capital. *Management Research Review*, 44(4), 607–624. <https://doi.org/10.1108/MRR-03-2020-0130>
 30. Keelan, C. M., Schenk, A. M., McNally, M. R., & Fremouw, W. J. (2014). The Interpersonal Worlds of Bullies. *Journal of Interpersonal Violence*, 29(7), 1338–1353. <https://doi.org/10.1177/0886260513506278>
 31. Kim, K. Y., & Choi, J. S. (2021). Cyberbullying, student nurses' ethical awareness and the Covid-19 pandemic. *Nursing Ethics*, 28(7–8), 1258–1268. <https://doi.org/10.1177/09697330211010280>

32. Kim, Y., & Choi, J. S. (2021). Individual and organizational factors influencing workplace cyberbullying of nurses: A cross-sectional study. *Nursing & Health Sciences*, 23(3), 715–722. <https://doi.org/10.1111/nhs.12858>
33. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. <https://doi.org/10.1037/a0035618>
34. Kowalski, R. M., & Limber, S. P. (2007). Electronic Bullying Among Middle School Students. *Journal of Adolescent Health*, 41(6 SUPPL.), 22–30. <https://doi.org/10.1016/j.jadohealth.2007.08.017>
35. Kowalski, R. M., & Limber, S. P. (2013). Psychological, Physical, and Academic Correlates of Cyberbullying and Traditional Bullying. *Journal of Adolescent Health*, 53(1), S13–S20. <https://doi.org/10.1016/j.jadohealth.2012.09.018>
36. Kumar, V., & Sadeeq, M. (2020). Estimation Of Psychometrics Of Cyber Bullying Attitude Measure In Indian Context. *European Journal of Molecular & Clinical Medicine*, 7(6), 2880–2887.
37. Li, Q. (2006). Cyberbullying in Schools. *School Psychology International*, 27(2), 157–170. <https://doi.org/10.1177/0143034306064547>
38. Macpherson, L. (2022). *The Psychological Experience of Cyberbullying Among Transgender Adults*. Walden University.
39. Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007). The relative importance of online victimization in understanding depression, delinquency, and substance use. *Child Maltreatment*, 12(4), 314–324. <https://doi.org/10.1177/1077559507305996>
40. Moore, P. M., Huebner, E. S., & Hills, K. J. (2012). Electronic Bullying and Victimization and Life Satisfaction in Middle School Students. *Social Indicators Research*, 107(3), 429–447. <https://doi.org/10.1007/s11205-011-9856-z>
41. Ndiege, J. R. A., & Kanyi, P. W. (2018). Cyberbullying in institutions of higher learning in developing countries: Evidence from Kenya. *2018 IEEE International Symposium on Technology and Society (ISTAS)*, 108–112. <https://doi.org/10.1109/ISTAS.2018.8638267>
42. Ngo, A. T., Tran, A. Q., Tran, B. X., Nguyen, L. H., Hoang, M. T., Nguyen, T. H. T., Doan, L. P., Vu, G. T., Nguyen, T. H., Do, H. T., Latkin, C. A., Ho, R. C. M., & Ho, C. S. H. (2021). Cyberbullying Among School Adolescents in an Urban Setting of a Developing Country: Experience, Coping Strategies, and Mediating Effects of Different Support on Psychological Well-Being. *Frontiers in Psychology*, 12. <https://doi.org/10.3389/fpsyg.2021.661919>

43. Nikolić, D., Čizmić, S., Vukelić, M., Tošković, O., Damnjanović, K., & Lazarević, L. (2017). Workplace cyberbullying and employee emotional well-being: The moderating effect of perceived organisational support. In O. Tošković, K. Damnjanović, & L. Lazarević (Eds.), *Zbornik radova sa XXII naučnog skupa Empirijska istraživanja u psihologiji*, 24-26. mart 2017. (pp. 133–137). Filozofski fakultet, Univerzitet u Beogradu.
44. Olenik-Shemesh, D., Heiman, T., & Eden, S. (2012). Cyberbullying victimisation in adolescence: Relationships with loneliness and depressive mood. *Emotional and Behavioural Difficulties*, 17(3–4), 361–374. <https://www.learntechlib.org/p/88471/>
45. Park, M., & Choi, J. S. (2019). Effects of workplace cyberbullying on nurses' symptom experience and turnover intention. *Journal of Nursing Management*, 27(6), 1108–1115. <https://doi.org/10.1111/jonm.12779>
46. Peluchette, J. V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? *Computers in Human Behavior*, 52, 424–435. <https://doi.org/10.1016/j.chb.2015.06.028>
47. Saman, Z. M., Siti-Azrin, A. H., Othman, A., & Kueh, Y. C. (2021). The Validity and Reliability of the Malay Version of the Cyberbullying Scale among Secondary School Adolescents in Malaysia. *International Journal of Environmental Research and Public Health*, 18(21), 11669. <https://doi.org/10.3390/ijerph182111669>
48. Schenk, A. M., & Fremouw, W. J. (2012). Prevalence, Psychological Impact, and Coping of Cyberbully Victims Among College Students. *Journal of School Violence*, 11(1), 21–37. <https://doi.org/10.1080/15388220.2011.630310>
49. Schenk, A. M., Fremouw, W. J., & Keelan, C. M. (2013). Characteristics of college cyberbullies. *Computers in Human Behavior*, 29(6), 2320–2327. <https://doi.org/10.1016/j.chb.2013.05.013>
50. Schneider, S. K., O'donnell, L., Stueve, A., & Coulter, R. W. S. (2012). Cyberbullying, school bullying, and psychological distress: A regional census of high school students. *American Journal of Public Health*, 102(1), 171–177. <https://doi.org/10.2105/AJPH.2011.300308>
51. Shapka, J. D., & Maghsoudi, R. (2017). Examining the validity and reliability of the cyber-aggression and cyber-victimization scale. *Computers in Human Behavior*, 69, 10–17. <https://doi.org/10.1016/j.chb.2016.12.015>
52. Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry and Allied Disciplines*, 49(4), 376–385. <https://doi.org/10.1111/j.1469-7610.2007.01846.x>

53. Snyman, R., & Loh, J. (2015). Cyberbullying at work: The mediating role of optimism between cyberbullying and job outcomes. *Computers in Human Behavior*, 53, 161–168. <https://doi.org/10.1016/j.chb.2015.06.050>
54. Somma, A., Gialdi, G., Arioli, C., De Ciechi, A., Mariani, V., & Fossati, A. (2022). Assessing cyberbullying in adolescence: Psychometric properties and external correlates of the Cyberbullying Experience Scale in Italian community-dwelling adolescents. *Behaviour & Information Technology*, 1–13. <https://doi.org/10.1080/0144929X.2022.2045360>
55. Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., Ristkari, T., & Helenius, H. (2010). Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents. *Archives of General Psychiatry*, 67(7), 720–728. <https://doi.org/10.1001/archgenpsychiatry.2010.79>
56. Souza, S. B., Veiga Simão, A. M., Ferreira, A. I., & Ferreira, P. C. (2018). University students' perceptions of campus climate, cyberbullying and cultural issues: implications for theory and practice. *Studies in Higher Education*, 43(11), 2072–2087. <https://doi.org/10.1080/03075079.2017.1307818>
57. Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, 4(1), 71–92. <https://doi.org/10.1177/14614440222226271>
58. Stewart, R. W., Drescher, C. F., Maack, D. J., Ebesutani, C., & Young, J. (2014). The development and psychometric investigation of the cyberbullying scale. *Journal of Interpersonal Violence*, 29(12), 2218–2238. <https://doi.org/10.1177/0886260513517552>
59. Tanrikulu, I., & Erdur-Baker, Ö. (2021). Psychometric properties of a Cyberbullying Inventory for university students. *British Journal of Guidance & Counselling*, 49(3), 494–507. <https://doi.org/10.1080/03069885.2020.1775174>
60. Tian, L., Yan, Y., & Huebner, E. S. (2018). Effects of Cyberbullying and Cybervictimization on Early Adolescents' Mental Health: Differential Mediating Roles of Perceived Peer Relationship Stress. *Cyberpsychology, Behavior, and Social Networking*, 21(7), 429–436. <https://doi.org/10.1089/cyber.2017.0735>
61. Topcu, Ç., & Erdur-Baker, Ö. (2018). RCBI-II: The Second Revision of the Revised Cyber Bullying Inventory. *Measurement and Evaluation in Counseling and Development*, 51(1), 32–41. <https://doi.org/10.1080/07481756.2017.1395705>
62. Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2018a). When workplace bullying goes online: construction and valida-

- tion of the Inventory of Cyberbullying Acts at Work (ICA-W). *European Journal of Work and Organizational Psychology*, 27(1), 28–39. <https://doi.org/10.1080/1359432X.2017.1363185>
63. Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2018b). Kicking someone in cyberspace when they are down: Testing the role of stressor evoked emotions on exposure to workplace cyberbullying. *Work & Stress*, 32(4), 379–399. <https://doi.org/10.1080/02678373.2018.1437233>
 64. Vranjes, I., Erreygers, S., Vandebosch, H., Baillien, E., & De Witte, H. (2018). Patterns of cybervictimization and emotion regulation in adolescents and adults. *Aggressive Behavior*, 44(6), 647–657. <https://doi.org/10.1002/ab.21790>
 65. Walker, C. M., Sockman, B. R., & Koehn, S. (2011). An Exploratory Study of Cyberbullying with Undergraduate University Students. *TechTrends*, 55(2), 31–38. <https://doi.org/10.1007/s11528-011-0481-0>
 66. Zhang, D., Huebner, E. S., & Tian, L. (2020). Longitudinal associations among neuroticism, depression, and cyberbullying in early adolescents. *Computers in Human Behavior*, 112, 106475. <https://doi.org/10.1016/j.chb.2020.106475>
 67. Zhang, H., Sun, X., Chen, L., Yang, H., & Wang, Y. (2020). The Mediation Role of Moral Personality Between Childhood Psychological Abuse and Cyberbullying Perpetration Attitudes of College Students. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.01215>
 68. Zhang, S., Leidner, D., Cao, X., & Liu, N. (2022). Workplace cyberbullying: A criminological and routine activity perspective. *Journal of Information Technology*, 37(1), 51–79. <https://doi.org/10.1177/02683962211027888>
 69. Zhang, Z., Wang, H., Zhang, L., & Zheng, J. (2021). Workplace cyberbullying and interpersonal deviance: roles of depletion and perceived supervisor support. *Asia Pacific Journal of Human Resources*. <https://doi.org/10.1111/1744-7941.12303>

SAJBERBULING I SAJBER VIKTIMIZACIJA: PREGLED LITERATURE O INSTRUMENTIMA ZA PROCENU²

Tokom poslednje dve decenije, naše znanje o sajber nasilju i njegovim posledicama je povećano. Detaljniji uvid u karakteristike sajberbulinga i sajber viktimizacije je moguć uz značajno raznovrsne mere procene. Međutim, ne postoji usaglašenost o najboljoj metodi merenja. Ovaj pregled literature je imao za cilj da identifikuje i predstavi instrumente i mere procene koje su konstruisane i korišćene za procenu sajberbulinga i/ili sajber viktimizacije. Ukupno 2031 publikacija je identifikovano sistematskom pretragom. Proces selekcije je rezultirao sa 11 instrumenata procene koji su dalje analizirani. Prema nalazima, polazna tačka u sastavljanju ili adaptiranju instrumenata za procenu specifičnih za naš kontekst treba da bude konzistentna, poboljšana i standardizovana definicija sajberbulinga uporediva sa definicijama koji se koriste širom sveta, praćena preciznim kriterijumima za reprezentativnost ciljne populacije i pažljivo razmotrenim socio-kulturalnim faktorima i utvrđenim vremenskim okvirom.

KLJUČNE REČI: sajberbuling / merenje / procena / sajber uznemiravanje

² Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)

THE INCREASE IN DOMESTIC VIOLENCE DURING THE CORONAVIRUS PERIOD: WITH SPECIAL FOCUS ON CHILDREN POSITION

Katalin CSEPREGI¹
István KOVACS, PhD²

The focus of this paper is on protecting children from domestic violence. Domestic criminal law (Hungarian) has contributed to the criminalization of domestic violence, and it protects not only women but also children. The authors conducted a statistical analysis of data collected during the coronavirus period. Statistical analysis includes a comparison of data on domestic violence during the coronavirus and two years before this period. The authors examine whether there was an increase in domestic violence, especially violence against children, during the coronavirus period. Restrictive measures (confinement or curfew) and psychological reactions have been identified as some of the leading causes that contribute to the increase in domestic violence.

KEY WORDS: child protection / domestic violence / child protection system / criminal law / coronavirus

¹ Master's Degree Student (MSc.), Faculty of Political Science and International Studies, National University of Public Service, Hungary cskata9@gmail.com

² Assistant Professor, Faculty of Law Enforcement, University of Public Service, Hungary, kovacs.istvan@uni-nke.hu

1. INTRODUCTION

The coronavirus epidemic has plagued the countries of the world, which has resulted in expressive health and social aspects. Many countries have suppressed and limited the control of the virus and its spread through official measures. Authorities and government measures have extended the restrictions to all areas of life.

Restrictions affected everyday routine activities (shopping), education (digital nature of public education), private activities (acquaintance), work (working from home), and the exercise of human and constitutional rights (right to move).

The psychological effects of quarantine or working from home occurred in a short time and significantly increased the escalation of workload conflicts.

Cohabitation at 0-24 hours, stress at work, feelings of insecurity, and questioning the viability of the future have led to intra-family conflicts and, in many cases, domestic violence. Moreover, the victims of the violence were women and children. (Frech Á., 2020: 1-3).

This research paper highlights the issue of domestic violence during the coronavirus period, with a particular focus on the situation of children. The research carried out in the study examines the crime of “relationship violence” in the Criminal Code in force in Hungary during the period of the coronavirus and analyzes its official statistics. The analysis is complemented by a comparative study that can determine the difference between crimes committed during the coronavirus and the “peacetime” period.

The research methodology is a statistical analysis obtained from the Criminal Statistics System from a public register. The subject of the research focused in particular on violence against children in the context of circumstances caused by the coronavirus. We hypothesize an increase in crime during the coronavirus period, which may be indirectly related to coronavirus-related restrictions.

2. THEORETICAL OUTLOOK ON RELATIONSHIP/DOMESTIC VIOLENCE

On 17 September 2012, based on a popular initiative, the Parliament passed a resolution on domestic violence regulation as an independent criminal law fact. Within the Ministry of Justice, with the involvement of professional and non-governmental organizations, a committee was set up to draft the law, considering the relevant international conventions on combating and preventing violence against

women and domestic violence. Section 212 / A of our current Penal Code provides for the facts of domestic violence, which can be read as follows (Act C of 2012, The Hungarian Penal Code):

“212 / A. § (1) A person who is a parent of a child, or a relative living in the same household or in an apartment with him or her at the time of the commission or earlier, to the detriment of his or her former spouse, former partner, guardian

a) commits a serious violation of human dignity, humiliation and violence,
b) deprives the victim of material assets belonging to joint management or common property, thereby rendering the victim severely deprived,

if a more serious crime is not committed, the offense is punishable by up to two years' imprisonment.

(2) Who regularly acts to the detriment of a person specified in subsection (1)

a) for endangering body pursuant to Section 164 (2) or defamation pursuant to Section 227 (2), for three years,

b) bodily harm pursuant to Section 164 (3) and (4), violation of personal liberty pursuant to Section 194 (1) or coercion, from one to five years

shall be punishable by a term of imprisonment.

(3) It is also possible to ban a perpetrator of domestic violence.

(4) The offense referred to in paragraph 1 shall be punishable only on the private motion”.

There is a recognizable pattern in domestic violence. Some forms of emotional, spiritual terror, physical, criminal, and sexual violence occur in the abuse process. Isolation of the victim from the environment decreases self-confidence, and verbal abuse is widespread. The goal is to weaken the victim's personality, increase vulnerability, and increase fear. Violence can take an increasingly harsh, perpetrating form, with abuse often leading to injury but simultaneously threatening the victim not to dare to seek help, not being allowed to go to the doctor, and often being restricted in their freedom of movement.

Forms of violence are verbal, physical, psychological, sexual and financial; here are some examples:

Cases of verbal abuse: humiliation, insult, ridicule, threats of abuse, beatings, abduction of children, suicide.

Cases of psychological violence: Refusal of basic emotional needs and demands, isolation or prohibition from friends, work, family, favorite activities, jealousy, systematic destruction of self-confidence, constant blaming, denial of telephone and other communication channels, the permanent control by telephone.

Cases of physical violence: Pushing, slapping, strangling, kicking, biting, burning, threatening or hurting with a weapon (knife, firearm, heavy objects), refusing basic physical needs and necessities (starvation, thirst, deprivation of sleep), closure, and restrictions on freedom of movement.

Cases of sexual violence: coercion into unwanted sexual activity, rape, pain or humiliation of sex, abuse of intimate parts of the body, coercion to have sex with others.

Cases of economic (financial) violence: material dependency, dismissal or disqualification, misappropriation of a woman's salary, questioning daily expenses and accounting for pennies (Makó K., 2017: 1-5).

3. THE RESEARCH

The research is based on the publicly available Criminal Statistics System, in which we analyzed and evaluated the crime of partnership violence during the coronavirus period. The results obtained are compared with the domestic violence crimes committed during the "peacetime period," and findings are made that are suitable for confirming or rejecting the hypothesis.

Today in Hungary, there is a zero-tolerance policy on domestic violence. If the child is abused, that immediately entails criminal liability (Gergely A., 2020: 1-39). The basis of the research was provided by the database of the Criminal Statistic System (in Hungarian: Bűnügyi Statisztikai Rendszer, BSR). The System collect statistics in many categories. It is a public register that covers the period from 2013 to 2022 and can represent data on the sex and age of the victims, the place where the crime was committed, and the perpetrators. As a result stated above implied, we also calculated maximum, minimum and average value resulted in the performance of mathematical-statistical tests.

3.1. Research results

We aimed to get a comprehensive picture and an overview of the Hungarian situation regarding domestic violence, particularly against children. We were curious about how much the number of cases has increased during the pandemic. Moreover, we want to know the typical characteristics of perpetrators and victims. We relied on our publication's hypotheses and Hungarian bibliography about the topic. The data was analyzed related to the restrictions of the pandemic; therefore, we highlight two time periods. We analyzed four years - from 2018 and 2021, but the comparison was made for 2018-2019 and 2020-2021. In order to depict the tendencies, diagrams were made in various forms.

Defining the periods was connected to the pandemic and its restrictions. In January 2020, the Operational Task Force for Coronavirus Epidemic Control entered into force (Koronavírus-járvány Elleni Védekezésért Felelős Operatív Törzs), which started to meet daily as the situation got worse and worse in the country. On 11 March, the government announced a state of emergency. People mainly went to the home office, and home education and rules on mask use were also tightened. On 27 March, a curfew was introduced, meaning people could only leave their homes with a good reason. After 2020, we can talk about the second, third, and even fourth waves of the pandemic, causing more and more challenges for the people to adapt. Staying home was not beneficial for all the people; particular ongoing problems have increased. This special order meant a more significant threat to the victims of domestic violence and eventually led to an increased number of them. At the same time, civil organizations suffered from challenges never seen before. COVID-19 has changed the whole dynamic of families. The role of professionals, doctors, teachers, and social workers dealing with children has grown. Their job is based on fundamental social interactions and connections, which were completely changed during the past months. (Francsics F. et al., 2020: 78-82) This non-precedent event put even more pressure on children, deepening the differences and the process of polarization (Gyarmathy É., 2021: 1-20).

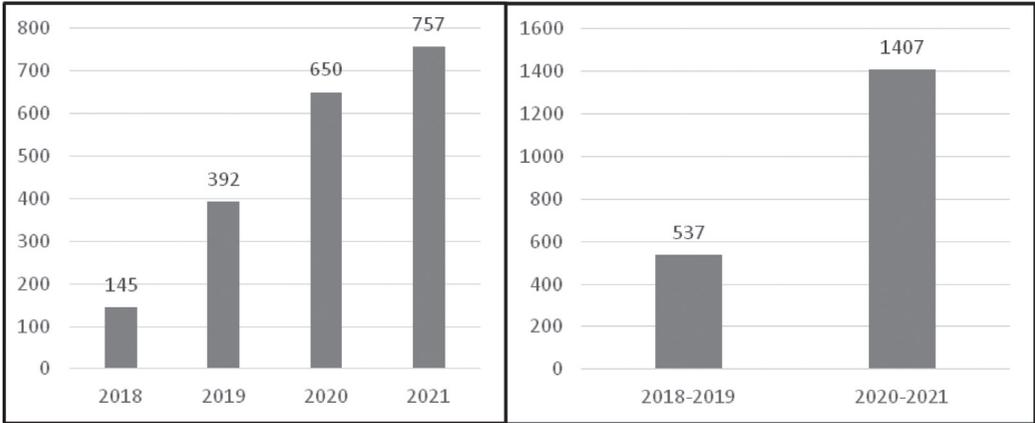


Table 1: Registered cases of domestic violence in Hungary depicted in four years separately and in two-year periods

The registered cases of domestic violence have increased fivefold during the four years. The change in the number growing from 145 to 757 can be explained on the one hand by the work of the police and authorities, whose improvements affect the efficiency of dealing with domestic and relationship violence. That is likely to bring more cases to the attention of the authorities; they can take bet-

ter action against the crime. However, the increased number of cases means that the country has more and more cases. The latency regarding domestic violence is extremely high. In the second diagram (Table 1), the two time period can be seen compared. The growth is more than doubled. There is an increase of 2.6 times, meaning that in “peacetime,” 537 cases were registered, but in the pandemic, even 1407.

After the general statistics of domestic violence, we focused more on the characteristics of the perpetrators. The primary hypothesis is that domestic violence is committed primarily by men. It is essential to underline that domestic violence against children can be committed not only by parents but also by grandparents, brothers, sisters, cousins, step-parents, and other relatives (Pintér Á. et al., 2017: 847-872).

Putting these two diagrams next to each other below can be deceptive (Table 2). Both examine the two years, but one belongs to the men’s tendencies, and the other is the women’s. Both are showing rapid growth, but the numbers are pretty different. The number of male offenders increased from 341 to 972, an almost threefold increase, while the number of female offenders increased from 10 to 65, a sixfold increase.

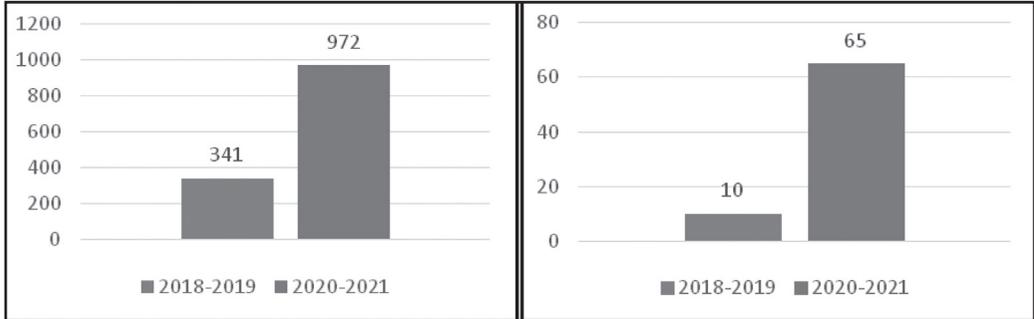


Table 2: Number of male perpetrators (left) and number of female perpetrators (right)

Unfortunately, the characteristics of the perpetrators committing domestic violence against children cannot be analyzed because there is no distinguished data or filter for that. However, we saw it necessary to show these numbers and features to better understand the crime’s tendencies.

We examined the perpetrators’ age and did not get surprising results. The following diagram (Table 3) shows that most perpetrators are between 25 and 59, even though this age group is extensive and contains several very different generations. They are followed by a younger age group between 18 and 24; lastly, older people come after them, with age above 60.

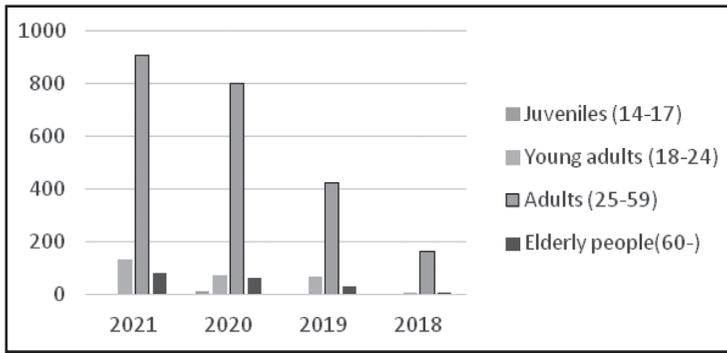


Table 3: Age groups of the perpetrators

We also found it essential to look at the gender ratio for the victim statistic. Even though the common stereotype lives vividly in our society, not only women and girls can be victims of domestic violence but also men and boys.

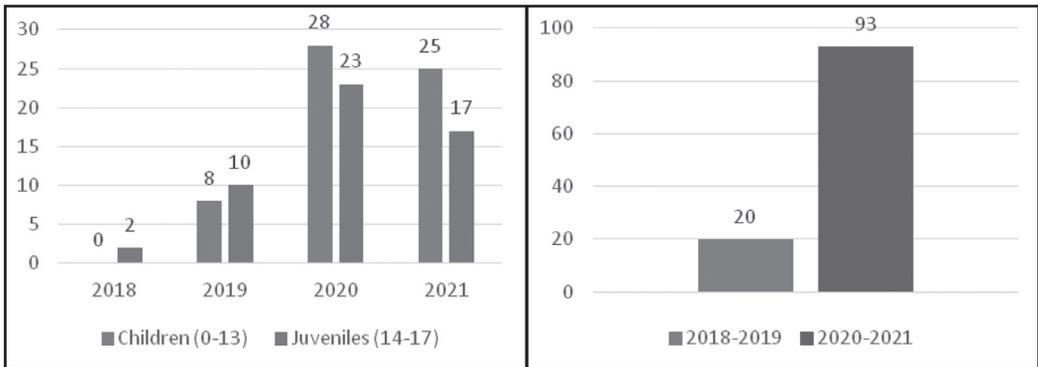


Table 4: Number of female victims between the ages of 0 and 17

The statistics of domestic violence against children show alarming figures on the diagrams. The ratio of victims, girls and boys, in 2021 compared to the pre-pandemic has increased fourfold. In 2018-2019 twenty victims were registered, but in 2020-2021, ninety-three victims. Among them, child age victims occur primarily between 0 and 13. In our previous publication called The online sexual exploitation of children, particularly the crime of child pornography, we reached a very similar result. According to that analysis, we have concluded that victims are more likely to be female than males, and their average age is 13 (Csepregi K. et al., 2022: 7-24). In connection with child pornography (which can also take part in domestic violence as a threatening tool against children), two specific victim groups were determined: juveniles between the ages of 15-18 were primarily victims of prostitution or coercion for prostitution. The younger ones between the ages of 7-13 were victims of domestic violence committed by a stepfather, uncle, or other rela-

tives. Unfortunately, it is a general but truthful saying that girls are the most vulnerable group to sexual violence (Antal J., 2020: 1-54).

Examining the statistics of boys was surprising because their growth ratio was even more radical. Before the pandemic, only nine young victims were registered. After that, by 2021, this number was 59. It is more than six-fold growth. The tendency that children have higher chances to become victims than juveniles is also visible here.

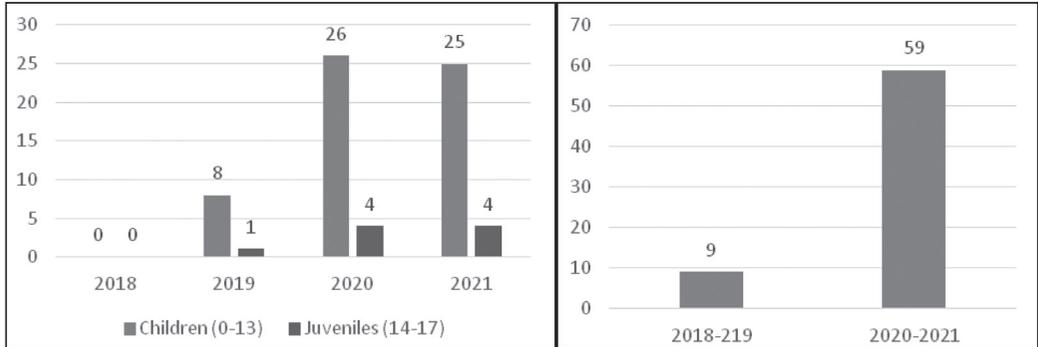


Table 5: Number of male victims between the ages of 0 and 17

Finally, we decided to look at the geographical indicators of the cases and analyzed the data in the aspect of the counties in Hungary. Most victims were from the western part of the country; Csongrád county stood out, followed by Komárom-Esztergom, Somogy, and Veszprém. The illustration should be treated as unexpected, as it is a popular misconception that domestic violence is only a problem for the poor and the non-intellectuals when, like any crime, it can happen to anyone, regardless of background.

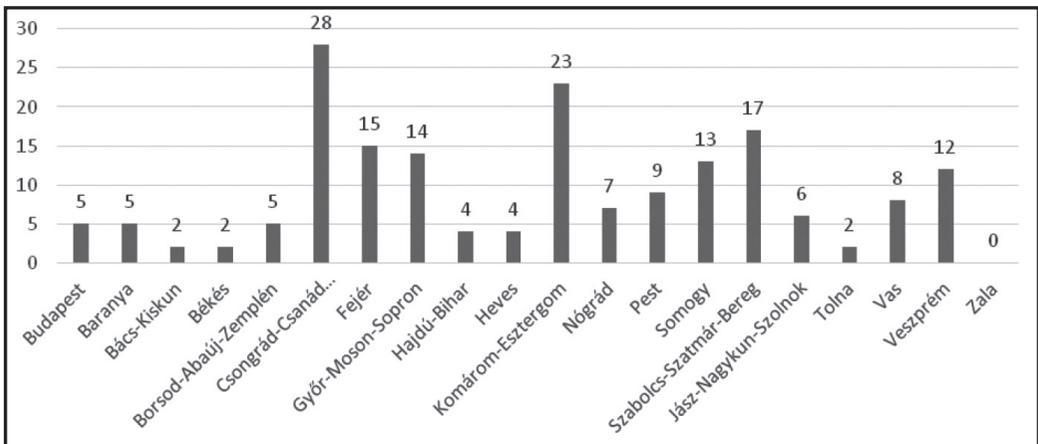


Table 6: Distribution of victims of domestic violence between the ages of 0-17 in Hungary

To summarize our results, we can conclude that, in general, domestic violence has grown more than 2.6 times from the beginning of the pandemic. Within this, the number of cases related to minors as victims has grown five times during the pandemic. The proof of our hypothesis was successful; data shows how the registered cases changed during these four years. The central figures about gender distribution and the rapidness of changes are alarming. The COVID-19 pandemic has changed our everyday lives upside down, to which we have to adapt and take action to reduce domestic and relationship violence in Hungary.

4. THE SITUATION IN HUNGARY, RECOMMENDATIONS AND SUMMARY OF THE PAPER

Proof of the hypothesis was only possible in part; no direct link could be established between the measures taken and the statistical indicators. However, it is indisputable and confirms the hypothesis that the number of investigated crimes tripled and sometimes quadrupled during the coronavirus period, unlike during peacetime. An increase was detectable in each of the categories examined. This increase was not a simple and low quantity but a qualitative and high increase. Unfortunately, it was impossible to carry out further investigations, which would have explained the reasons by a detailed study of the statistical cases (for example, interviewing). All of this encourages researchers to conduct such studies in the future. It is indisputable that the source-critical analysis also revealed that the restrictive measures may have been responsible for the increased number of cases, all due to underlying personality and psychological reasons. (For example, feelings of seclusion, hopelessness, fear, etc.) For the above reasons, however, we summarize the conclusions below, which could also be drawn from the statistics, and make forward-looking suggestions.

Compared to Western countries, Hungary started to address the issue of domestic violence relatively late, in the 1970s (Antal J., 2020: 1-54). In the 1990s, these countries started to put children the focus of fighting against domestic violence by creating more mental hygiene and advocacy services for them. They realized how important it is to invest in children's physical and mental development.

In Hungary, domestic violence is considered to be catch-all phenomenon, and therefore child abuse is traditionally subsumed under this concept. Common belief according to the public is that authorities only take action when it is already

too late. As a result, the term has become synonymous with violence against women, to the detriment of the treatment of violence against children (Gyurkó Sz., 2009: 329-346).

Dealing with a crisis, for example, with the rising figures of domestic violence, is possible essentially in two ways: individually and socially. In the first one, responsibility is on the individual itself, and the state can intervene only as a last resort.

However, if we consider the problem a social crisis, the responsibility lies with the state. Therefore, the state's attitude towards families, children, and violence itself indicates its values and priorities on the issue. The measures taken can be supportive and helpful but also controlling, punitive, and restrictive (Kerezsi K., 1995: 1-182). That can also be described as the more liberal a country's policies on families, and social policy are, the more responsibility they take for their external policies. However, if the regulations are fixed and strict, the responsibility is constantly shifted towards the individual, leaving them alone with their solutions. For a long time in the past, Hungary has reinforced the second tendency, the consequences of which are still being felt today.

What influences the well-being of a family and, at the same time, the amount of stress they experience depends mainly on the particular economic circumstances. With crises, social support is often withdrawn, cutting off avenues and institutions that were previously a lifeline. Indirectly, these contribute to an increase in domestic violence, the further marginalization of the most disadvantaged, and the widening of social gaps (Kerezsi K., 1995: 1-182). The economic situation contributes indirectly to family dynamics. Moreover, the advantages and disadvantages of social status can be passed down through generations. In addition to economic conditions, the political situation in the country is of particular importance. Politics influences the place and role of the family in society. It impacts the everyday decisions of the family, the motives of their actions, and what customs and habits are learned. The successive reassessment of the tasks and functions of the family according to current political criteria each time results in a new situation and, most of all, makes the norm-transmitting function of the family vulnerable (Kerezsi K., 1995: 1-182). An excellent example of this is an examination of juvenile delinquency data. Indeed, the ever-increasing numbers can be attributed to a dysfunctional family and the pattern it imposes on children. The biggest problem is that there are no parenting patterns and methods generally accepted by Hungarian society. While in the 1990s, the world started to pay more and more attention to stopping violence against children, in Hungary, the police only dealt with the shortcomings. The backlog that has developed persists nowadays. In the

2000s, crime statistics did not reflect the experience of civil organizations, especially child protection organizations. In Hungary, there is still a dubious reception for adults who dare to speak publicly about domestic violence suffered in childhood (Herczóg M., 2005: 77-92). Moreover, it was considered a complete taboo topic (Kibicher O., 2003: 1-10). A case is only brought to the public on many occasions when it is too late. However, it is necessary to present cases publicly, reinforcing the importance of prevention in people's minds. Physical and psychological abuse within the family is a severe social problem.

We believe that a complex, well-functioning, and comprehensive system would be able to tackle the crime of domestic violence. That was attempted in the Methodological Guidelines for the Operation of the Child Protection Detection and Indication System (Módszertani Útmutató: A gyermekvédelmi észlelő- és jelzőrendszer működtetése kapcsán), published in 2017 by the Ministry of Human Capacities and the Directorate General for Social Affairs and Child Protection. It set out sector-neutral uniform principles and methodology for detecting and eliminating child abuse (GYÉJR, 2017: 1-60).

The child protection signposting system is a step forward from past practices. Whereas the authorities were characterized by passivity and symptomatic treatment until the 2000s, the signaling system has allowed for a redefinition of the problem and thus the development of a more comprehensive response. "Members of the child protection referral system have a statutory duty to monitor and address child vulnerability, particularly to identify and report child abuse and neglect cases to child welfare services." (Pintér Á. et al., 2017: 847-872.)

The system's effective functioning is provided by the first step focusing on prevention. It aims to look for the signs that lead us to recognize and suspect any atypical behavior (GYÉJR, 2017: 1-60). In case of suspicion, it is crucial to have someone to report to the police, and many civil organizations run helplines and provide advice and counseling. After further analysis of the situation, actual actions are planned, involving the authorities or other bodies. Finally, they will follow up, extend measures if necessary, or try to help in other ways. The methodological guide contains operational guidelines for public education institutions, the health sector, guardianship authorities, law enforcement agencies, and various social, child welfare, and child protection services.

We consider the work of the child protection signaling system to be necessary. However, for it to be effective, a high level of cooperation, a more coherent implementation of actions, and a proper legal background would be essential. According to professionals, the system is now unable to work to its potential because of the incomplete and inadequate detection of handling cases (Pintér Á. et

al., 2017: 847-872). After an initial boost, the field is now facing a shortage of human and other resources, overburdening the system and leading to insufficient attention being paid to cases that have already been detected. The pandemic did not help these tendencies; it cut fundamental relations and connections and set back progress.

As far as we are concerned, alongside the work of all the essential legal, public authority, public education, health, social and civil organizations, there is a need for a change in society itself, family attitudes, and individual responsibility. Prejudices that proclaim that there is a place for domestic violence against children must be combated. (Kibicher O., 2003: 1-10.) Signs of a problem must be identified and made widely known. Even greater emphasis must be placed on corrective action, on the intervention of mentally and psychologically prepared law enforcement workers. In addition, education should also play a role in preparing people for their role as parents and promoting a better understanding of family and social processes. Prevention is crucial, as in many cases, the abusive parent has experienced similar abuse as a child and, as a result, carries the patterns they have seen and experienced into their family dynamics.

The latency rate for violence against children is the highest of all crimes. The figures recorded and presented in the statistics are likely to be a fraction of the reality. Data collection on child abuse is significantly hampered by the high latency of the phenomenon, which may also be contributed to by the isolation mentioned above of families in the community, the prohibition of reporting the abuse suffered by the abuser, and the social reluctance to intervene in the internal affairs of families (Kerezsi K., 1995: 1-182). At the same time, the number of reported cases of abuse is increasing year by year. Some research suggests that the latency rate is decreasing, but the actual number of children involved in abuse is increasing.

Quarantine has intensified the challenges of the past years and set back progress in fighting against domestic violence. The confinement and curfew have increased anxiety and created tensions. The greatest challenge of confinement was the absence and loss of external contact concerning domestic violence. The child, who had been regularly in the community, suddenly had to stay with his abusive parent(s) for many days. The simple logic can explain the increased violence that no one will see or notice the consequences (Gyarmathy É., 2021: 1-20).

Child abuse develops continuously; it does not become part of their daily lives overnight. These gaps need to be better bridged to be stopped at an early stage, and appropriate actions should be taken. Social responsibility is essential, and material things greatly influence children and juveniles social and

moral development and how parents relate to each other (Kerecsi K., 1995: 1-182; Kerecsi K. et al., 2009: 1-462).

In Hungary today, the most complex and largest providers of assistance are civil society organizations. The NANE, Women Together Against Violence (Nőkért Együtt az Erőszak Ellen), focuses specifically on victims of domestic violence and has been assisting at the individual, community, and social levels not only women but also children since 1994. They operate an anonymous, free helpline, which should be called not only after an assault has occurred, but also at the first warning signs or even if someone is unsure. They also work with the Patent Association (Patent Egyesület), which fights against violence against women and supports networks and shelters. Their website provides accurate and reliable sources of information on abuse. Their campaigns, legal advice, cooperation with the authorities, social media, and publications help to ensure that victims get the help they need to start a new life and prevent domestic violence from developing and escalating.

There are also more and more opportunities for children to understand, recognize abuse, and dare to ask for help. In Hungary, one of the most active children's civil organizations is the Blue Line Children's Crisis Foundation (Kék Vonal Gyermekválság Alapítvány), which aims to present all forms of abuse and violence to children clearly and understandably. As they are also increasingly present on social media platforms, there is a greater chance that the information will reach the people who need it.

Our research has collected various data about domestic violence, particularly against children in Hungary, and given an overview of the current situation and its challenges. With the help of governmental strategies, documents, Hungarian bibliography, other useful sources we could get closer to the reality of the leftovers and consequences of the pandemic. For Hungary, the most important thing at this stage is to maintain the collective thinking and the improving tendency that started before the pandemic. Permanent and active cooperation between all actors is essential in developing child protection, social, education, health, law enforcement, and judicial services. The biggest lesson of the epidemic is the enormous growth of the online space, which, if used well, can bring many benefits to this fight. The Internet offers a chance to reach out to those in need and inform a more significant part of society. Domestic violence is a social problem, but it requires individuals to be socially sensitive. Awareness and preparedness can save children's lives and change generations so that the family can be a genuinely loving and protective community, not a place of the most brutal violence (Kerecsi K., 1995: 1-182).

REFERENCES

1. Act C of 2012, The Hungarian Penal Code. Source: <https://net.jogtar.hu/jogszabaly?docid=a1200100.tv> (Downloaded: 2022.04.01.)
2. Antal J. (2020): Családon belüli erőszak. Nők sérelmére elkövetett testi sértés. Miskolc: Miskolci Egyetem Állam- és Jogtudományi Kar, 1-54. o.
3. Csepregi K. et al. (2022): Online sexual exploitation of children, in particular the crime of child pornography, *Journal of Criminology and Criminal Law, Serbian Association for Criminal Law Theory and Practice*, 1. szám, 7-24. o.
4. Emberi Erőforrások Minisztériuma, Szociális és Gyermekvédelmi Főigazgatóság (2017): Módszertani Útmutató. A gyermekvédelmi észlelő- és jelzőrendszer működtetése kapcsán a gyermek bántalmazásának felismerésére és megszüntetésére irányuló szektorsemleges egységes elvek és módszertan. 1-60. o. Source: <https://kk.gov.hu/download/e/60/c0000/A%20gyermek%20b%20C3%A1ntalmaz%20C3%A1s%20C3%A1nak%20felismer%20C3%A9s%20C3%A9re%20C3%A9s%20megsz%20BCntet%20C3%A9s%20C3%A9re%20ir%20C3%A1nyul%20C3%B3%20egys%20C3%A9ges%20elvek%20C3%A9s%20m%20C3%B3dszertan.pdf> (Downloaded: 2022.03.05.)
5. Francsics F. et al. (2020): Körkép: Változások a szociális szférában a Covid-19 járvány idején: Interjúrészletek családsegítésben, lakásotthonokban, hajléktalanellátásban és időotthonban dolgozó szociális szakemberekkel. *Szociális Szemle*, 1. szám, 78-82. o.
6. Frech Á. (2020): A kapcsolati erőszak törvényi szabályozása és annak érvényesülése. *Belügyi Szemle*, 1-3. o. Source: <https://belugyiszemle.hu/hu/node/578> (Downloaded: 2022.03.20.)
7. Gergely A. (2020): Családon belüli erőszak: abuzált, bántalmazott gyerekek. Miskolc: Miskolci Egyetem Állam- és Jogtudományi Kar, 1-39. o.
8. Gyarmathy É. (2021): A COVID-19-járvány hosszabb távú pszichológiai hatásai – különös tekintettel a gyerekekre. *Magyar Tudományos Akadémia*, 6. szám, 1-20. o.
9. Gyurkó Sz. (2009): Gyermekbántalmazás, veszélyeztetett gyermekek. A kriminálpolitika és a társadalom bűnmegelőzési kézikönyve. Budapest: Igazságügyi és Rendészeti Minisztérium, 329-346. o.
10. Herczog M. (2005): A gyermekek elleni erőszak más megközelítésben – a bántalmazó rendszer. *Belügyi Szemle*, 9. szám, 77-92. o.

11. Kerezi K. (1995): A védtelen gyermek (Erőszak és elhanyagolás a családban). Budapest: Az Országos Kriminológiai és Kriminalisztikai Intézet Tudományos Kiadványai, 1-182. o.
12. Kerezi K. et al. (szerk.) (2009): A kriminálpolitika és a társadalmi bűnmegelőzés kézikönyve. Budapest: Fresh Art Design Kft., 1-462. o.
13. Kibicher O. (2003): Erőszak a négy fal között. Miskolc: Miskolci Egyetem Bölcsészettudományi Kara tudományos diákköri közleményei, 1-10. o.
14. Makó K. (2017): Családon belüli erőszak. Webüggyvédi fórum, 1-7. o. Source: <https://webugyved.com/csaladon-beluli-eroszak/> (Downloaded: 2022.03.05.)
15. Pintér Á. et al. (2017): A bántalmazott gyermekek – Gyermekekjogok és gyermekbántalmazás. Statisztikai Szemle, 8-9. szám, 847-872. o.

Katalin Csepregi, MSc
Nacionalni univerzitet javnih službi, Budimpešta, Mađarska

Prof. dr István Kovacs
Pravni fakultet, Univerzitet javnih službi, Budimpešta, Mađarska

NASILJE U PORODICI ZA VREME PANDEMIJE VIRUSA COVID-19 SA POSEBNIM OSVRTOM NA NASILJEM NAD DECOM

Fokus rada je na zaštiti dece od nasilja u porodici. Domaće (mađarsko) krivično pravo doprinelo je kriminalizaciji nasilja u porodici, i ono štiti ne samo žene, već i decu. U ovoj studiji autori sprovode statističku analizu podataka prikupljenih u periodu korona virusa. Statistička analiza obuhvata poređenje podataka o nasilju u porodici za vreme korona virusa, kao i dve godine pre ovog perioda. Autori ispituju da li je u periodu korona virusa došlo do porasta nasilja u porodici, a posebno nasilja prema deci. Kao neki od uzroka koji doprinose porastu nasilja u porodici prepoznati su restriktivne mere (zatvaranje i policijski čas) i psihološke reakcije koje su posledica ovih mera.

KLJUČNE REČI: zaštita dece / nasilje u porodici / sistem zaštite dece / krivično pravo / korona virus

PARENTAL MEDIATION IN THE AGE OF DIGITAL TECHNOLOGIES: HOW TO PREVENT A CHILD BECOMING CYBERBULLYING VICTIM

Hajdana GLOMAZIĆ, PhD¹
Katarina GLOMAZIĆ, MA²

The issue of protecting children from Internet abuse cannot be viewed outside the importance of the parental role in that process. In this paper, we investigate the relationship between parental mediation and child abuse through digital technologies. The aim of this paper is to examine whether parental mediation is a factor in reducing the risk of child abuse in the Internet space and whether intervention programs are designed to meet the needs of different categories of parents. The results have shown that parental mediation is a factor in preventing and reducing the risk of children online abuse. The extent of its success, among other factors, depends on the parental style and parental warmth. Furthermore, the data we have obtained suggest that it is necessary to deepen the current research on parental mediation in order to create better policies and program prevention.

KEY WORDS: cyberbullying / children online abuse / parental mediation / parental control / family support

1. INTRODUCTION

Technological changes in the modern world have led to the increased use of new technologies - the Internet as well as mobile and digital devices. Thus, the use

¹ Research Associate, Institute of Criminological and Sociological Research in Belgrade, hajdana.ng@gmail.com

² NVIDIA, Reading, United Kingdom, kglomazic26@gmail.com

of information and communication technologies in business and private contexts have become an integral part of everyday practice, and the transition from offline to online communication has particularly expanded during the COVID-19 crisis (Rodríguez-Rivas, Varela, González & Chuecas, 2022) establishing new rules in various spheres of life, work, and even parenting.

In addition to the positive changes brought about by technological innovations, we shouldn't overlook the negative impact caused by the abuse of the opportunities they provide. The data indicates that children, even at a younger age, are users of the Internet and online platforms, and the use of digital technology often takes place without parental control. Leaving children in an uncontrolled digital space without parental control carries numerous risks – therefore, such behaviour can result in their abuse in various ways. The spectrum of risks is large, as we are witnessing different types of fraud and criminal activities mediated by internet technologies. However, studies have shown that the extent of children's use of the Internet and the prevalence of risks have not yet been sufficiently investigated. To date, the data are fragmented and do not offer a large amount of opportunities for comparison between countries (Ivanović and Marković, 2017).

Nevertheless, what the authors do agree on, and what numerous studies point to, is the fact that violence against children in the digital environment can have considerable consequences for their mental health. The consequences of violence can be insecurity, withdrawal, increased anxiety, symptoms of depression, and even the risk of suicide. A worrying discovery is that there is a significantly higher risk of self-harm among children who have in some way been part of online abuse compared to children who have experienced other forms of violence (Rodríguez-Rivas et al., 2022; Nguyen, Nakamura, Seino & Vo, 2020).

One of the ways to act preventively and avoid negative consequences of children's communication on the Internet is parental mediation. It has been shown that the issue of violence on the Internet, whether children are victims or perpetrators of violence, cannot be viewed outside of parental control, partially due to its complexity and partially due to the fact that it involves the inclusion of a systematic approach to problem solving.

By internet, cyber and online violence we refer to all forms of violence that arise from the use of digital technologies. It takes place via computers, Internet, social networks, messaging applications, gaming platforms, mobile phones and other electronic devices. The characteristic of such a deliberate pattern of aggression is that it is repetitive and aims to frighten, anger or embarrass those who are attacked (Rodríguez-Rivas et al., 2022; UNICEF, 2021).

Parental mediation or parental intervention is defined as “different ways in which parents / guardians try to influence how and for what purposes their children use digital media” (Blum-Ross & Livingstone, 2016: 9).

2. DIGITAL TECHNOLOGIES AND VIOLENCE AGAINST CHILDREN

According to the data available to us, it can be seen that, in general, the number of Internet users is increasing rapidly. It is indicated that by December 2020, 55% of the world's population and 85% of Europe's³ population had access to the Internet. One third of those who are Internet users are children and young people under the age of 18 (Kuzmanović, Zlatarović, Andjelković and Žunić Cicvarić, 2019a). Recent research shows that in the United States, almost all young people have access to the Internet, meaning that 95% of adolescents in the United States are in the digital space between the ages of 12 and 17. They spend a large amount of their time (as much as 7.5 hours a day) using various digital technologies, out of which one quarter of the time is spent utilizing several forms of media at the same time. Furthermore, 74% of them access the Internet via mobile phones, tablets and other mobile devices (Elsaesser, Russell, Ohannessian & Patton, 2017). At the same time, the limit determining the appropriate age when children can start using the Internet has lowered, meaning that children at an even younger age use the Internet, often without parental mediation (Kuzmanović, Pavlović, Popadić and Milošević, 2019b).

When it comes to Serbia, the data has shown that in December 2020, there were 73.7% of Internet users, which is close to the European average⁴. The majority of the youth population in Serbia (86%) uses the Internet on a daily basis. At the age of 15-17, young students⁵ access the Internet every day from their smartphones (98%), while the percentage for children aged 9 to 10 is lower – 65% (Kuzmanović et al., 2019b). Young people in Serbia spend about 3 hours on average on the Internet; those in an older age (up to 17 years) spend 4 and a half hours a day, and on the weekends up to 7 hours (two thirds of them), with content mostly being related to entertainment, communication and social networks. Children and youth in Serbia are present on social networks in high percentage (74%). Of concern is data implying that 41% of children aged 9-10 and 72% of children aged 11-12 have an open account on social network(s), regardless of the fact that the age limit is regulated by social networks in a way that only makes it possible to open an account from the age of 13. What is interesting is that social networks among young people are not used for any form of civic activism, campaigns promotion for the youth and the like (ibid.).

³ See: <https://www.internetworldstats.com/stats4.htm#europe>

⁴ See: <https://www.internetworldstats.com/europa2.htm#rs>

⁵ Students participating in the research

In Europe, 46% of Internet users aged 9-16 have at least one risk of online violence in their experience. At the age of 9-10, this risk was at 17%, and with older age, the risk of violence on the Internet has increased accordingly to as much as 69%, for children aged 15-16 (Duerager & Livingstone, 2012). According to El-saesser et al. (2017), many studies have shown that online violence is widespread among young people, with 75% of school-age children experiencing online bullying at least once a year. In Chile, a sample of students from sixth to eleventh grade have shown that 8% of them suffered 9 or more types of aggression, with this type of violence being defined as poly-victimization of the victim. Among this group, 69% of them stated that they suffered from cyberbullying (Rodriguez-Rivas et al., 2022). Kuzmanović et al. (2019b) state that their research done in Serbia found that during one year, every third child experienced some form of harassment on the Internet. Most often, it was children aged 13-14 who had disturbing experiences.

Research has shown that young people exhibit risky behaviour online by sharing their personal information with strangers, making friendships from online ones to the ones in person, and by hiding behind personal profiles. In addition, they are exposed to sexual and pornographic contents, and data suggest that every other student has accessed sexual and pornographic content during the year. A large percentage of children were exposed to harmful content on the Internet (over 50%), such as those portraying violence against people, animals, hate messages, hate speech, self-destructive behaviours, content that encourages anorexic and bulimic behaviours, different ways of using drugs, and even contents that show in which way is it possible to commit suicide (44% of girls and 36% of boys were exposed to such contents) (Kuzmanović et al., 2019a and Kuzmanović et al., 2019b). Examples of direct violence in the Internet space to which children and young people are exposed include spreading untruths or false information, posting private photos and videos of someone on social networks (often sexualized), making threats and blackmailing through digital platforms, or false representation and harassment through sending inappropriate messages to others in someone else's name.

In summary, according to the authors, risky behaviours in the digital space can be divided into 3 groups: "content that children may be exposed to while using the Internet, which is unpleasant, disturbing or intimidating for the child; contacts with unknown people via Internet that can abuse a child in various ways and the child's behaviour in a digital environment that can endanger primarily personal safety, but the safety of family members and other persons (eg peers) as well" (Kuzmanović et al., 2019: 30-31).

Abuse on the Internet does not exclude real life violence, and they can often happen in parallel. According to some authors, violence in real life and internet violence have similar negative psychological and health consequences for victims over time, while others believe that the consequences of cyber violence are more adverse due to special hotspots of this phenomenon (Rodriguez-Rivas et al., 2022). However, one of the differences is that “violence on the Internet leaves a digital record that can serve as an evidence whilst in the process of putting an end to it” (UNICEF, 2021)⁶. The consequences of violence can last a long time and manifest themselves in different ways. Representations of these consequences can be feelings of threat, anxiety, depression, increased destructiveness and self-destructive behaviour, feelings of shame, physical symptoms of illness, health problems and chronic stress. Exposure to digital violence is associated with depression and low self-esteem (UNICEF, 2021), and among the most serious consequences of digital violence are suicides among young people. This has been reported by various studies; thus, it is suggested that the consequences of internet violence are related to the increase of suicidal ideation among young people (Hinduja & Patchin, 2010 according to Rodriguez-Rivas et al., 2022).

However, in the context of children’s development and their socialization, we believe that it would be beneficial to consider the findings of the *Children of Europe on the Internet* study, which, according to the authors, has shown that risks for children present in the digital space do not always result in negative consequences (Kuzmanović et al., 2019). That is, isolating children from the digital space, which is inevitably surrounding them, can have an impact on preventing the development of digital skills, as well as creating resistance to dangers in the digital space. Due to its complexity, this particular issue of risky behaviour should be approached very carefully without taking extreme positions in the form of banning the use of different types of digital technologies or absolute concessions and non-selective approach to the use of digital technologies. In fact, it would be extremely important to work on prevention (ibid.).

3. PARENTAL MEDIATION AND PREVENTION OF THE RISK OF CHILD ABUSE IN THE INTERNET SPACE

Parental mediation is an integral part of planning activities aimed at protecting children in the digital space. It is not a one-dimensional concept and includes both oversight and support. In the literature, various terms are used for this pro-

⁶ <https://www.unicef.org/serbia/zaustavimo-digitalno-nasilje>

cess, such as: parental mediation, monitoring, supervision, control, however, they mainly refer to the parents' behaviour aimed at protecting children from violence in the Internet space. Literature describes parental mediation as different types of parental behaviour that have an impact on the way children will use digital media (Blum-Ross & Livingstone, 2016) or is defined as "different ways parents try to influence on how and for what purposes their children are using digital media" (Blum-Ross & Livingstone, 2016: 9). Parental supervision is seen as a combination of rules, monitoring, communication and control of children when accessing Internet content and is primarily understood as a protection measure (Martín-Criado, Casas and Ortega-Ruiz, 2021). Some authors state that parental control involves behaviours used by parents to reduce inappropriate or risky behaviours of children and youth, including involvement in violence and victimization (Beck, Boile, & Boekeloo, 2003; Lac & Crano, 2009 according to Elsaesser et al., 2017). European Commission's documents which provide recommendations for the use of parental control tools on the Internet, define parental control tools as activities that increase the safety of children on the Internet, blocking, preventing, filtering and reporting on certain behaviours of children in the digital environment (European Commission, 2017). However, the recommendations emphasize that parental control tools cannot replace communication with children and youth and should be used in partnership with children through open dialogue and transparent communication (European Commission, 2017:5). Moreover, the document states that different functionalities of parental control tools are only part of the solution, so the focus should be on properly informing and educating young people, as well as children-parents cooperation in terms of spending time together in different types of activities.

Therefore, by parental mediation we do not refer to the literal use of a set of measures and mechanisms which would limit the Internet for children and youth, a restrictive, technical control, but rather child care in a way that allows mutual communication, preventive action and reducing the risk of harmful consequences in the digital space for children and youth.

The "warmth" dimension of parental mediation has been shown to be positively correlated with a reduction in risky online behaviour (Elsaesser et al., 2017; Rodriguez-Rivas et al., 2022) – thus, it is said that parental acceptance have shown a significant association with absence of self-harm and suicidal behaviour (Nguyen et al., 2020). In general, parental warmth and support are fundamentally important for the development of children and young people and they are positively correlated with their later achievements (academic, drug abuse, greater psychological adjustment) since they create a sense of security and safety for children (Elsaesser et

al., 2017). Similar observations have been found in other studies that emphasize the importance of family emotional support which makes the child feel protected and cared for (Arato et al., 2021; Rees et al., 2020; Fanti et al., 2012; Kovalski et al., 2014; Martins et al., 2016; Wang et al., 2009 according to Rodriguez-Rivas et al., 2022). From the perspective of cyber violence level, this leads to decrease in cyber-victimization, greater ability to balance emotions and resist bullying on the Internet, as well as lesser participation in cyberspace violence (Georgiou, 2008; Ok, Melahat Halat, & Aslan, 2010 according to Elsaesser et al., 2017).

Martín-Criado, Casas and Ortega-Ruiz (2021) state that some studies have addressed the issue of parenting style and online violence and have concluded that those in families who nurture open communication with children provide security and build a relationship of trust with children, therefore reducing the possibility of children's risky Internet communication on the Internet. On the other hand, children living in families with an authoritarian and careless parenting style, especially if there is an element of corporal punishment, are at higher risk of violence in the digital space and are more likely to become the perpetrator. The authors add that victimization is associated with a permissive parenting style (*ibid.*).

4. PARENTAL STRATEGIES IN THE PREVENTION OF VIOLENCE IN THE DIGITAL SPACE

Parents use different strategies to control what their children do while they're being online. Some research indicates that more active parental involvement in controlling children's behaviour on the Internet is associated with more frequent restrictions, although these findings vary depending on the country and culture to which they belong. That is, the northern European countries (Norway, Sweden, Denmark, Finland and the Netherlands) actively mediate and control children's behaviour on the Internet, however, their control style is not restrictive, on the contrary – it is below average. On the other hand, the countries of Eastern Europe (Lithuania, Estonia and Romania) are characterized by below-average active and restrictive mediation. Furthermore, in Austria, Italy and Belgium, the style of parental control is restrictive with less active participation in monitoring children's behaviour in the digital space compared to the European average. Parents in some southern European countries and the largest European countries (Portugal, Spain and Greece, France, Germany and the UK) use highly active and highly restrictive mediation, i.e. control (Duerager & Livingstone, 2012). Research has shown that parents in Serbia rarely use child control mechanisms online and to a lesser extent

than in other countries. Less than half of the sample of children and young people aged 9 to 17 (44%) say that their parents often explain how to use the Internet safely, and slightly more than a third of children said that their parents talk to them about what they do online (Kuzmanović et al. , 2019).

According to the authors, in a large number of studies, parental mediation focuses on its four forms: active (parents are actively involved in children's activities on the Internet); restrictive (parents restrict the use of Internet) and parental supervision or monitoring (parents monitor what children do in the digital space) (Kuzmanović et al. 2019a).

The risks that children may be exposed to while they are online can be reduced by using active parental mediation, using open communication with children about these topics while they are offline, or by being close to children while they are online. Additionally, restrictive mediation has been shown to be associated with risk reduction, while technical mediation shows no effect in reducing online risk at any age (Duerager & Livingstone, 2012).

Studies have shown that parental behaviour can be related to certain characteristics such as education, age, ethnicity, digital competence, parents' knowledge of online bullying, parental competence in this regard, attribution of parental responsibility, parental perception of online risk, or family supervision. When examining the reliability of instruments that measure parental awareness and supervision to prevent cyberbullying, it was found that there were differences relating to parents' age, child's school level and parents' level of education for the dimensions of parental competence and parental supervision (Uslu & Durak, 2022). Martín-Criado et al (2021) assessed positive parental involvement through several variables: parents' knowledge of online bullying, perceptions of parental competence in this regard, parental perceptions of online risk, and attribution of parental responsibility in digital education. Hereby, the results have shown that positive parental involvement can be predicted if parents are more aware of online violence, if parenting competencies are stronger, when there is better risk adaptation and if they accept parental responsibility (Martín-Criado et al., 2021). In addition, lower levels of parental awareness regarding the importance of communication relating to children's behaviour in the digital space are associated with greater inactivity or neglect (ibid.)

5. DISCUSSION

The Internet space, apart from the regular ones, is sometimes overloaded with various security-problematic and criminal activities. Such digital space is availa-

ble to children who are not able to recognize the risks they may face, and, as a consequence, they become involved in a network of online violence, either as a victim or a perpetrator. At the systemic institutional level, ways to protect children from online violence are regulated by numerous legal solutions and documents adopted at national and international levels. It should be noted that they are only part of the solution to this problem.

As mentioned, numerous research and studies addressing the topic of violence through digital technologies that affect children and youth, have shown that there is no comprehensive solution to this issue without involving parents in the process. As we have previously stated, literature most frequently describes parental behaviour in this process as parental mediation. However, there are often different terms in the literature that are used to describe the same parental behaviour, such as: parental control, parental supervision, parental mediation, parental monitoring. The impression is that there is still a terminological inconsistency when it comes to the behaviour of parents whose goal is to protect their child from the potential risks in the Internet space. Additionally, different terms are used in digital literature, so cyberspace, digital, online, virtual, internet, etc., usually refer to the same space online. In this paper, we have used these terms as synonyms, since defining them individually in the theoretical sense would not be relevant for the purpose of this paper.

In an attempt to answer the central question in this paper, which refers to the actions parents can take to protect their children from becoming either a victim or a perpetrator of violence on the Internet, we had some interesting findings. Namely, as suggested by research data, basic principle in preventing children from becoming victims or bullies, and which refers to parents is: their awareness and knowledge about this problem as well as emotional warmth (Rodriguez-Rivas et al., 2022; Martín-Criado et al., 2021; Nguyen et al., 2020; Elsaesser et al., 2017). Studies have shown that parents of adolescents who did not use restrictive mediation underestimated the extent to which their child witnessed violence in the digital world – because of this possible underestimation, the importance of parental knowledge and awareness of negative online behaviour in childhood and adolescence is particularly emphasized (Caivano, Leduc & Talwar, 2020). Parents' knowledge of the ways in which internet violence is perpetrated and their concerns could be the drivers of parental mediation.

If there is sufficient support, care for the child and sense of security and safety in the parental atmosphere and family overall, the chances to avoid risks are higher.

Furthermore, a key point in parental mediation is preferred parental style. The best results are given by the type of monitoring which includes conversation and open supportive communication, as well as parents' active participation and supervision of children's online activities.

Parents are mostly educated about the use of technologies for the purpose of restrictive action, thus, it may be said that they have limited knowledge regarding digital violence and the techniques they can use to prevent it. Parents who have higher digital competencies do not achieve particularly positive effects in terms of child protection, since it is considered that solely technical restrictions without an open access show either minimal effects or none at all. According to researchers, parental competence is the most important and influential factor for involvement in parental supervision; greater involvement can generally be expected in situations where a parent has knowledge of cyberbullying.

“It must be understood, consequently, that a positive parental involvement can be predicted from high scores in knowledge and perception of competence; from a parental adjustment in the appreciation of online risks and from a suitable attribution of parental responsibility to assume guidance and control in this new field of digital education. On the contrary, the attribution of the responsibility exclusively to the school, together with the ignorance or alienation of the social–digital life of their children, seem to be indicators of risk. It follows that families need to deepen their knowledge about online relationships and the risks they imply, but also to assume their own responsibility to intervene in this area of education. These conclusions are in line with current research that points out the importance for parents to know strategies of positive and safe parental mediation in the digital education of their children (Martín-Criado et al., 2021:11).”

6. CONCLUSION

With respect to the above, there is no doubt that parental prevention is extremely important when it comes to protecting children from the violence mediated by digital technologies and preventing violence against children and youth in the Internet space. However, as we have shown, there are certain limitations in terms of insufficient research data exploring the extent to which parents have knowledge and awareness of what Internet violence is and how they can protect their children from it.

There are only a few studies in the literature that have investigated this issue from the parental aspect in terms of their competencies, awareness of the importance of the problem, the prevalence of the phenomenon, their value orientations and their attitudes on this issue. In that sense, it is necessary to further investigate this phenomenon. As some authors say, “for a whole generation of parents, cyberbullying prevention is a new educational task to be developed at home. Today, given the current levels of connectivity, this task has taken on renewed urgency” (Martín-Criado et al., 2021: 11). Accordingly, the data obtained from the research could serve to better predict family involvement in the prevention of digital violence, create mechanisms to measure their involvement in prevention and assess the current quality of interventions, as well as develop more concrete measures for intervention.

Additionally, to date, studies have shown that parental involvement in prevention and their interventions can vary according to their education, age, ethnicity, and the characteristics of the culture to which they belong. It is recommended to deepen current research in order to assess how can these factors shape parental behaviour related to internet violence.

Lastly, prevention programs rich in technical guidelines for controlling children’s behaviour on the Internet can be frustrating for parents of lower education and could be a factor in giving up involvement in the process of parental mediation – instead, they can be supplemented with other interventions that will be more receptive to parents and which would help them “educate and protect their children” (Martín-Criado et al., 2021: 11). In this sense, it is necessary to supplement the existing policies and programs with new, adapted education programs for parents that will be designed in a way that is accessible and understandable to them.

REFERENCES

1. Blum-Ross, A. & S. Livingstone (2016) *Families and screen time: Current advice and emerging research*. Media Policy Brief 17. London: Media Policy Project, London School of Economics and Political Science. Available at: <http://eprints.lse.ac.uk/66927/1/Policy%20Brief%2017-%20Families%20%20Screen%20Time.pdf> page accessed 30.04.2022.
2. Caivano, O., Leduc, K., & Talwar, V. (2020) When you think you know: The effectiveness of restrictive mediation on parental awareness of cyberbullying experiences among children and adolescents. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 14(1), Article 2. <https://doi.org/10.5817/CP2020-1-2>

3. Duerager, A. & Livingstone, S. (2012) *How can parents support children's internet safety?* London: EU Kids Online. Available at: https://www.researchgate.net/publication/313011658_How_can_parents_support_children's_internet_safety/link/588c8d31a6fdcc8e63c94f3f/download page accessed 24.04.2022.
4. Elsaesser, C., Russell, B., Ohannessian & Patton, D. (2017) Parenting in a digital age: A review of parents' role in preventing adolescent cyberbullying. *Aggression and Violent Behavior*, (35), 62-72. <https://doi.org/10.1016/j.avb.2017.06.004>.
5. European Commission (2017) Benchmarking of parental control tools for online protection of children - Full Study on parental control tools for online protection of children Available at: <https://digital-strategy.ec.europa.eu/en/library/benchmarking-parental-control-tools-online-protection-children> page accessed 24.04.2022.
6. Ivanović, J. and Marković, D. (2017) Save the Children in the North West Balkans, *Mapa puta prevencije online i drugih nasilja nad decom na internetu u republici Srbiji*, Sarajevo: Amos Graf available at <https://www.pars.rs/images/biblioteka/visokotehnoloski-kriminal/Mapa-puta-prevention-online-i-drugih-nasilja-nad-decom-na-internetu-u-RS.pdf> page accessed 22.04.2022.
7. Kuzmanović, D., Pavlović, Z., Popadić D. and Milošević, T. (2019b) *Korišćenje interneta i digitalne tehnologije kod dece i mladih u Srbiji - Rezultati istraživanja Deca Evrope na internetu*. Belgrade: Institute of Psychology, Faculty of Philosophy in Belgrade. Available at: https://www.unicef.org/serbia/media/12511/file/koriscenje_interneta_i_digitalne_tehnologije_kod_dece_i_mladih_u_Srbiji.pdf page accessed 23.04.2022.
8. Kuzmanović, D., Zlatarović, V., Anđelković, N. and Žunić Cicvarić, J. (2019a) *Deca u digitalnom dobu*. Uzice: Uzice Center for Children's Rights. Available at: https://www.unicef.org/serbia/media/10366/file/Deca_u_digitalnom_dobu.pdf page accessed 23.04.2022.
9. Martín-Criado, J.M., Casas, J.A. & Ortega-Ruiz, R. (2021) Parental Supervision: Predictive Variables of Positive Involvement in Cyberbullying Prevention. *Public Health*, (18), 1562. <https://doi.org/10.3390/ijerph18041562>
10. Nguyen HTL., Nakamura, K., Seino K. & Vo, VT. (2020) Relationships among cyberbullying, parental attitudes, self-harm and suicidal behavior among adolescents: results from a school-based survey in Vietnam. *BMC Public Health*. 20 (1) 476. doi: 10.1186 / s12889-020-08500-3

11. Rodríguez-Rivas, M.E., Varela, J., J., González, C. & Chuecas, M. J. (2022) The role of family support and conflict in cyberbullying and subjective well-being among Chilean adolescents during the Covid-19 period. *Heliyon*, 8 (4), e09243. <https://doi.org/10.1016/j.heliyon.2022.e09243>.
12. UNICEF - What is digital violence and how to stop it? (2021) Available at: <https://www.unicef.org/serbia/zaustavimo-digitalno-nasilje> page accessed 22.04.2022.
13. Uslu, N. U. & Durak, H. Y. (2022) Parental awareness and supervision to prevent cyberbullying: Scale adaptation and a review in terms of demographic variables. *Children and Youth Services Review*, (133), 106329, <https://doi.org/10.1016/j.childyouth.2021.106329>.

Dr Hajdana Glomazić
Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

Katarina Glomazić, MA
NVIDIA, Velika Britanija

RODITELJSKA MEDIJACIJA U DOBA DIGITALNIH TEHNOLOGIJA: KAKO DA DECE NE POSTANE ŽRTVA NASILJA NA INTERNETU⁷

Pitanje zaštite dece od zlostavljanja u internet prostoru, se ne može posmatrati izvan značaja roditeljske uloge u tom procesu. U ovom radu se bavimo odnosom između roditeljske medijacije i zlostavljanja dece putem digitalnih tehnologija. Cilj rada je ispitivanje da li je roditeljska medijacija faktor smanjenja rizika od zlostavljanja dece u internet prostoru i da li su programi intervencije osmišljeni tako da odgovore potrebama različitih kategorija roditelja. Rezultati su pokazali da roditeljska medijacija jeste faktor prevencije i smanjenja rizika od zlostavljanja dece na internetu. U kojoj meri će biti uspešna, između ostalog, zavisi od stila roditeljstva i roditeljske topline. Takođe, podaci do kojih smo došli sugerišu da je potrebno produbiti dosadašnja istraživanja o roditeljskoj medijaciji kako bi se kreirale bolje politike i programi prevencije.

KLJUČNE REČI: zlostavljanje dece na internetu / sajber nasilje / roditeljska medijacija / roditeljski nadzor / porodična podrška

⁷ Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)

COMBATING CHILD SEXUAL ABUSE ONLINE IN EUROPEAN UNION AND THE GENERAL PROCESSING OF ELECTRONIC COMMUNICATIONS

Andela ĐUKANOVIĆ, PhD¹

The fight against child sexual abuse and exploitation is recognized as a priority for the EU, having in mind the significant increase in detected cases of online child sexual abuse in recent years. In order to resolve issue of online child sexual abuse, EU resorted to voluntary practice of processing online interpersonal communications by service providers, not based on firm legal basis. After extension of the scope of the Privacy and Electronic Communications Directive 2002/58/EC, this voluntary practice was paused, until the adoption of Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC. However, it seems that the imposed limitations on the right to private life and protection of personal data do not respect the essence of these rights, there was no detailed analysis of necessity and proportionality of general processing of content data and possible adverse effects on combating online child sexual abuse.

KEY WORDS: online child sexual abuse / private life / protection of personal data / Regulation (EU) 2021/1232 / electronic communications

1. INTRODUCTION

The fight against child sexual abuse and exploitation is recognized as a priority for the EU, having in mind the significant increase in detected cases of child sexual abuse in recent years.² In many cases, children are sexually abused by persons

¹ Research Fellow, Institute of Criminological and Sociological Research, andjelasto@sbb.rs

² COM(2020) 607 final, p. 1.

they know and trust, and on whom they are dependent. This makes these crimes difficult to prevent and detect, and there are indications that the COVID-19 crisis has exacerbated the problem, especially for children who live with their abusers (WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children, UNESCO, 2020:1).

Confidentiality of communications is an essential part of the right to private and family life and protection of personal data. In light of the significant increase in reports of child sexual abuse online over the last decade, the EU approved a controversial law that would allow digital companies to detect and report child sexual abuse on their platforms for the period of three years, without the fear of violating Europe's privacy laws.³ It will probably cease to be valid before this period, when the permanent regulation on subject is adopted. Temporary derogation was adopted because of the extended scope of the Privacy and Electronic Communications *Directive 2002/58/EC* (hereinafter: ePrivacy Directive) resulting from the entry into force of the European Electronic Communications Code Directive (hereinafter: EECC Directive) in December 2020.⁴ Providers of certain interpersonal communications services, such as webmail and messaging services, previously used specific technologies on a voluntary basis to detect online child sexual abuse on their services, and report it to law enforcement authorities. This activity was previously governed solely by Regulation (EU) 2016/679 (hereinafter: General Data Protection Regulation). However, this voluntary activities constituted an interference with the right for private and family life and to the protection of personal data of all users of number-independent interpersonal communications services, and cannot be justified merely on the grounds that providers were using certain technologies at a time when number independent interpersonal communications services did not fall within the definition of 'electronic communications services'.⁵ Protection of right to private life and personal data however is not absolute, and can be limited under certain circumstances.

2. EU STRATEGY IN COMBATING CHILD SEXUAL ABUSE ONLINE

The fight against child sexual abuse is recognized as a priority for the EU. As a result, EU adopted Strategy for a more effective fight against child sexual abuse, which should be implemented in the period of five years (2020-2025). Numbers

³ Official Journal of the European Union, L 274/41, 30.7.2021.

⁴ Official Journal of the European Union, L 201, 31.7.2002; Official Journal of the European Union, L 321, 17.12.2018.

⁵ Official Journal of the European Union, L 274/41, 30.7.2021, paras 7-8.

concerning the child abuse online in EU are truly alarming. Some analysis of child sexual abuse online in EU (e.g. images exchanged in the EU, victims in the EU, etc.), suggest that there is an increase from 23 000 reports in 2010 to more than 725 000 in 2019.⁶ It seems that the hosting of child sexual abuse URLs is almost exclusively located in Europe (90%), compared to other continents (Internet Watch Foundation, 2020). Also, there is an increase in number of URLs in 2020, compared to 2019 (Internet Watch Foundation, 2020). Interpol also reported increased sharing of child exploitation material through peer-to-peer networks during the COVID-19 pandemic (Interpol, 2020).

EU Strategy for a more effective fight against child sexual abuse, is aimed at full implementation of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography (hereinafter: Child Sexual Abuse Directive), adopted more than decade ago.⁷ At the same time, Strategy is directed at assessment of the Child Sexual Abuse Directive implementation in practice, in terms of effectiveness, efficiency, relevance, and particularly assessment of the online aspects of these crimes, where doubts exist as to whether the present framework is adequate after ten years of technological changes and the significant growth of online sharing.⁸

EU Strategy for a more effective fight against child sexual abuse also states that the use of encryption technology for criminal purposes needs to be immediately addressed through solutions which could allow companies to detect and report child sexual abuse in end-to-end encrypted electronic communications, which are beneficial for ensuring privacy, but also facilitate secure channels for perpetrators.⁹ The Commission has launched an expert process to find possible technical solutions to detect and report child sexual abuse in end-to-end encrypted electronic communications, and to address regulatory and operational challenges and opportunities in the fight against these crimes.¹⁰

3. REGULATION ON TEMPORARY DEROGATION

EECC Directive extended the scope of the e-privacy Directive to over the top (OTT) inter-personal communication services such as messenger services and email. The ePrivacy Directive does not contain a legal basis for voluntary process-

⁶ COM(2020) 607 final, p. 1.

⁷ Official Journal of the European Union, L 335, 17.12.2011.

⁸ COM(2020) 607 final, p. 6.

⁹ COM(2020) 607 final, p. 2.

¹⁰ COM(2020) 607 final, p. 16.

ing of content and traffic data for the purpose of detecting child sexual abuse. In the absence of legislative measures under the Article 15 of the e-privacy Directive, measures to detect child sexual abuse undertaken by these providers, which process content or traffic data, would lack a legal basis.¹¹

The US National Center for Missing and Exploited Children (NCMEC) showed a 46% drop of reports of EU child sexual abuse-related cases in the weeks after the European Electronic Communication Code entered into force compared to the previous weeks, as a direct consequence of the new EU privacy legislation (US National Center for Missing and Exploited Children). This had led to child rights and other human rights organizations to urge for adoption of a temporary derogation to the ePrivacy Directive (Eurochild, 2021). In July 2021, EU adopted Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of ePrivacy Directive as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (hereinafter: Regulation on temporary derogation). Regulation on temporary derogation is seen only as a temporary solution to fix an acute emergency, and there is a need for permanent answer to counter a persistent threat against children (European Commission, 2021). However, there are statements that the Swiss Federal Police found that in the vast majority of cases (86%), innocent citizens are reported for having committed an offence due to the unreliable technology (Betruzzi, 2021).

Regulation on temporary derogation provides for a temporary derogation from Articles 5(1) and 6(1) of ePrivacy Directive which protect the confidentiality of communications and traffic data.¹² EECC Directive extended the

¹¹ COM(2020) 607 final, p. 4. According to Article 15 of the e-privacy Directive, provided rights and obligations can be restricted if this is necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or in case of unauthorized use of the electronic communication system, Official Journal of the European Union, L 201, 31.7.2002, Article 15.

¹² Member States shall ensure the confidentiality of communications and the related traffic data, and particularly, prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with above mentioned Article 15(1), Official Journal of the European Union, L 201, 31.7.2002, Article 5 (1); “traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.” Official Journal of the European Union, L 201, 31.7.2002, Article 6(1).

definition of electronic communication services online. Under the EU law, number-independent interpersonal communications service represents “an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans”.¹³ This for an example includes popular services as Facebook Messenger, dating applications, emails or any other form of online communication that might develop. According to Regulation on temporary derogation, the term of ‘online child sexual abuse material’ encompasses definitions of child pornography, pornographic performance, and solicitation of children from Child Sexual Abuse Directive, and ‘online sexual abuse’ represents online child sexual abuse material and solicitation of children.¹⁴

Regulation on temporary derogation does not apply to the scanning of audio communications. Articles 5(1) and 6(1) of ePrivacy Directive do not apply to the confidentiality of communications involving the processing by providers of personal data, if certain conditions are met. This is possible if “processing is strictly necessary and proportionate for the use of specific technology for the sole purpose of detecting and removing online child sexual abuse material and reporting it to law enforcement authorities and to organizations acting in the public interest against child sexual abuse and of detecting solicitation of children and reporting it to law enforcement authorities or organizations acting in the public interest against child sexual abuse”.¹⁵

Compared to initial Proposal on temporary derogation, there is an extensive list of other conditions that must be met.¹⁶ The technologies used for the stated purpose, must be “in accordance with the state of the art in the industry and are the least privacy-intrusive”, and “to the extent that they are used to scan text in communications, they are not able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible online child sexual abuse”. Therefore, the scanning is strictly limited to detecting patterns, which is a significant improvement compared to initial Proposal on temporary derogation.

Also, in respect of any specific technology used, prior data protection impact assessment must be conducted, the technologies used must be sufficiently reliable

¹³ Official Journal of the European Union, L 321, 17.12.2018, Article 2(7).

¹⁴ Official Journal of the European Union, L 335, 17.12.2011, Article 2 (c), Article 2 (e) and Article 6.

¹⁵ Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (a)i.

¹⁶ COM/2020/568 final.

and limiting to the maximum extent possible errors, patterns of possible solicitation of children are limited to the use of relevant key indicators, and objectively identified risk factors such as age difference and the involvement of a child in the scanned communication.¹⁷ Providers are also obliged to ensure human oversight of and, where necessary, human intervention in the processing, to establish appropriate procedures and redress mechanisms, and to inform users of the fact that they have invoked the derogation.¹⁸ Where suspected online child sexual abuse has been identified, providers must report it to competent authorities without delay, block the account, or suspend or terminate the provision of the service, and to create a unique, non-convertible digital signature ('hash') of data reliably identified as online child sexual abuse material.¹⁹ The data is stored no longer than strictly necessary for the relevant purpose, but no longer than 12 months from the date of the identification.²⁰

File Hashing is the most elementary technology used to detect online child sexual abuse, used to automatically detect content and/or behaviors, the intermediate category is Computer Vision and the most innovative is Artificial Intelligence which is the most advanced type of artificial intelligence and can potentially cope with the most complex scenarios (Council of Europe, 2021). Regulation on temporary derogation does not include end-to-end encryption communication, however this may be the case in the planned long-term legislation, and the processing of data will probably be mandatory for the providers. End-to-end encryption represents a method of secure communication that prevents third parties from accessing data, meaning that only data sender and receiver are able to read the message. There are technologies that are able to access targeted data contained in end-to-end encryption, like the client-side scanning. This technology implies that every relevant device must have installed software that will monitor activities and alert authorities. However, this particular technology is being criticized as less secure for the users, prone to abuse from unauthorized or authorized parties, with possibility of false positive results (Abelson et al, 2021).

¹⁷ Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (c), Article 3 (e-f).

¹⁸ Where users content has been removed or their account has been blocked or a service offered to them has been suspended, to inform users of the avenues for seeking redress from them, and to provide possibility of lodging a complaint and the right to a judicial remedy, Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (f)i-vi.

¹⁹ Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (h)i-iii.

²⁰ Official Journal of the European Union, L 274/41, 30.7.2021, Article 1 (h)i.

4. INTERFERENCE WITH THE RIGHT TO PRIVATE AND FAMILY LIFE, AND THE PROTECTION OF PERSONAL DATA

Since the Regulation on temporary derogation recognizes that voluntary activities of Providers of interpersonal communications services in detection of online child sexual abuse represent an interference with the right for private and family life and to the protection of personal data (even before the entry into force of the EEC Directive), it is necessary to assess whether this interference is in accordance with Article 52(1) of the EU Charter of Fundamental Rights. Article 52(1) of the Charter sets out specific criteria that must be met by any legislation that seeks to limit the exercise of the rights and freedoms provided by the Charter. These criteria are that: 1) the limitation must be provided for by law; 2) it must respect the essence of the rights and freedoms; 3) Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.²¹ In addition, under a relatively new right to protection of personal data, such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.²² Usually, courts do not explore and interpret the right to protection of personal data independently from the right to private life, which is seen as a well-established fundamental right, and also, these right are closely linked (Pia & Bonnici, 2014: 142).

It must be noted that there was no impact assessment on fundamental rights for the initial Proposal. European Parliamentary Research Service (EPRS) issued Targeted substitute impact assessment afterwards, on request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (EPRS, 2021).

When it comes to legal basis of Regulation on temporary derogation, it is stated that "this Regulation does not provide for a legal ground for the processing of personal data by providers for the sole purpose of detecting online child sexual abuse on their services and reporting it and removing online child sexual abuse material from their services, but it provides for a derogation from certain provisions of Directive 2002/58/EC."²³ It is also stated that the Regulation on temporary derogation is based on Article 114 TFEU, which is very general in nature. Article 114 TFEU use as a legal basis is controversial, since it has been successfully challenged before the Court of Justice of the European Union (CJEU) on several occasions,

²¹ Official Journal of the European Union. C 326/391, 26.10.2012, Article 52 (1).

²² Official Journal of the European Union. C 326/391, 26.10.2012, 8 (2).

²³ Official Journal of the European Union, L 274/41, 30.7.2021, par. 10.

when the measures in question did not to fulfil the objectives on the establishment and functioning of the internal market (Wällgren, 2016: 5). Also, Regulation on temporary derogation is based on Article 16 TFEU which provides a “specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law”.²⁴ However, it is clear that processing of personal data is being carried by private actors, on voluntary basis.

In addition, Regulation on temporary derogation states that General Data Protection Regulation remains applicable to the processing of personal data.²⁵ According to General Data Protection Regulation, processing of personal data is possible if one out of six conditions set out in Article 6(1) is fulfilled.²⁶ It is evident that first two conditions are not applicable, that the data subject has given consent or that the processing is necessary for the performance of a contract (EPRS, 2021: 28-29). According to Opinion of European Data Protection Supervisor, since the derogation concerns voluntary processing of personal data, legal basis also cannot be found in Article 6(1)c of the General Data Protection Regulation, aimed at processing which is necessary for compliance with a legal obligation to which the controller is subject (European Data Protection Supervisor, 2020 §19). Article 6(1)e of the General Data Protection Regulation, which is directed at processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, is not a valid legal basis, since the controllers are not public authorities, and processing on this basis must be explicitly stated in Regulation on temporary derogation, which is not the case (EPRS, 2021: 30).

However, the voluntary practice of processing data in order to protect the vital interest set out in Article 6(1)(d) of the General Data Protection Regulation, might serve as legal basis. Relevant vital interests, are the interests of any child that might be the victim of online sexual abuse (EPRS, 2021: 29). Vital interest is defined as a “interest which is essential for the life of the data subject or that of another natural person”, however General Data Protection Regulation suggests that this basis should be used exceptionally, where the processing cannot be manifestly based on other legal basis, and sets out as an example humanitarian emergencies, in particular situations of natural and man-made disasters.²⁷

Finally, according to 6(1)(f) of the General Data Protection Regulation processing might be lawful if it is “necessary for the purposes of the legitimate inter-

²⁴ Official Journal of the European Union, L 274/41, 30.7.2021, par.15.

²⁵ Official Journal of the European Union, L 274/41, 30.7.2021, paras. 13-14, Article 1.

²⁶ Official Journal of the European Union, L 119, 4.5.2016. Article 6(1).

²⁷ Official Journal of the European Union, L 119, 4.5.2016, par 46.

ests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". However, these cumulative requirements need case-by-case balancing exercise, where the controller must ensure that the legitimate interests are not overridden by the interests or rights and freedoms of data subject which require protection of personal data" (EPRS, 2021: 31). This basis might be questionable when the processing is aimed at communication of every subject, and not targeted at possible suspects, and where controller is a private actor. Therefore, it can be concluded that the processing of personal data under the Regulation on temporary derogation, or voluntary processing that took place before entry into force of the EEC Directive, is/was based on a shaky legal ground.

Any restriction must respect the essence of the right that is being restricted, so the restrictions that are extensive and intrusive to the extent that they void a fundamental right of its basic content, cannot be justified. General exclusion of all user's rights with regard to all number-independent interpersonal communications, do not seem justified in this respect. European Data Protection Board was of this opinion in relation to application of restrictions of General Data Protection Regulation. General exclusion of all data subjects' rights with regard to all data processing operations as well as a general limitation of the rights of all users for specific data processing operations, shall be considered unlawful, even without the need to further assess whether it serves an objective of general interest or satisfies the necessity and proportionality criteria (European Data Protection Board, 2020: 6).

Interference with the right for private and family life and to the protection of personal data must meet: a) objective of general interest recognized by the EU, which is in this case the effective prevention, detection and prosecution of related crimes, the protection of victims may be identified as adequate, and b) the need to protect the rights and freedoms of others, in this case the right to such protection is necessary for their well-being of the child (EPRS, 2021: 32).

The interference with the right for private and family life and to the protection of personal data, also must be necessary and proportionate for achieving the objective, and answer to this question is not easy task. Necessity of some measure implies that the measure used, is the least intrusive for achieving one objective. As stated by the CJEU, in order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, that legislation must be legally binding under domestic law, and must indicate in under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly neces-

sary.²⁸ CJEU also stated that the need for such safeguards is all the greater where personal data is subjected to automated processing, and especially where the protection of the sensitive category of personal data is at stake.

There is no elaborate evidence on efficiency of the practice included in Regulation on temporary derogation in fighting sexual abuse online, and that there are no other less intrusive but effective measures. For example, this could lead to increased use of decentralized or encrypted channels of communications by offenders, and in general their effort to reach out from law enforcement authorities (EPRS, 2021: 34). It is highly likely that the practice of offenders will shift to other methods, although Regulation on temporary derogation will have the effect of making the commission of the crime more difficult. The Commission and EU Member States also did not provide information about the actual number of prosecutions and convictions that resulted from existing voluntary practices (EDRI, 2021).

In addition, Regulation on temporary derogation uses terms like “least privacy-intrusive”, that technologies used are “sufficiently reliable”, and limited to the use of “relevant key indicators”, with no further elaboration, except that the technology must not deduce the substance of the content of the communications, but detect patterns. Some of dilemmas might be resolved in future, since the European Data Protection Board will ensure the oversight of the scanning practices and technologies used, and prepare guidelines on which technologies could be used.²⁹

There was also no detailed analysis of the reliability of technology’s that can be used. Automatic scanning by algorithms of all chat conversations and emails, of all users, without court order or any initial suspicion, can lead to errors, which might further lead to private content being analyzed by private company employees and police authorities. EU is relying on technologies managed by private US organizations, and encouraging them in surveillance of the sensitive personal data.

According to Opinion of European Data Protection Supervisor, general, indiscriminate and automated, analysis of all text-based communication with an aim of identifying new infringements does not respect the principle of necessity and proportionality, even with additional safeguards (EDPS, 2020 §26). Any interception of private communications must target only the person or persons under investigation, and not all users of the service, based on specific, reasonable, individual level suspicion, and any investigation of private communications must be specifically and individually warranted by a judge (EDRI, 2022). European Parliamen-

²⁸ *La Quadrature du Net and Others v Premier ministre and Others*, ECLI:EU:C:2020:791, par. 132.

²⁹ Official Journal of the European Union, L 274/41, 30.7.2021, Article 4.

tary Research Service was also against the use of these techniques to monitor all private messages, but to be limited to private messages of persons under suspicion of soliciting child abuse or distributing online child sexual abuse material (EPRS, 2021: 47). The CJEU, retreated that the general and indiscriminate retention of traffic and location data, and the particularly serious interference constituted by the automated analysis of that data, can meet the requirement of proportionality only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine, present or foreseeable, and if the duration of that retention is limited to what is strictly necessary.³⁰

Council of Europe Convention on Cybercrime (*Budapest Convention*) seems directed at traffic data, and the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication.³¹ Convention on Cybercrime addresses the subject of real-time collection and recording of traffic data, but for the purpose of specific criminal investigations or proceedings. However, Article 21 of the Convention on Cybercrime is directed to collection or recording of "content data" in real-time, in relation to serious offences determined by domestic law. Term of content data is not defined in Convention on Cybercrime (Baron, 2002: 277). Explanatory Report to the Convention on Cybercrime indicates that this term refers to the content of communication. The conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data.³² Importantly, Convention on Cybercrime is directed at "specified communications" (Articles 20-21). Therefore, the Convention does not require or authorize the general or indiscriminate surveillance and collection of large amounts of traffic data, where criminal activities are hopefully sought to be detected, the judicial or other order authorizing the collection must specify the communications to which the collection of traffic data relates.³³ For example, measures from the recently adopted Second Additional Protocol to the Convention on Cybercrime, apply only to specific criminal investigations and proceedings, and do not entail general communications surveillance.³⁴

³⁰ *La Quadrature du Net and Others v Premier ministre and Others*, ECLI:EU:C:2020:791, par. 177.

³¹ Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, par. 29.

³² Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, par. 231;

³³ Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, par. 219.

³⁴ Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CM(2021)57-final, 17 November 2021.

EU and Member States' responses to serious problem of combating online child sexual abuse must invest in prevention, education, victim support, social services, welfare and other methods of addressing the root causes of the issues, and the technological fixes are not solution to complex societal problems (EDRI, 2022). Many Member States faced delays in the implementation of the Child Sexual Abuse Directive into their national law. EU Strategy for a more effective fight against child sexual abuse, recognizes existing challenges in areas of prevention, criminal law, and assistance, support and protection measures for child victims.³⁵

In light of the EU accession negotiations of Republic of Serbia, there is no reaction in relation to the implementation of Regulation on temporary derogation. This might be the case since the adoption of permanent legislation is expected in near future. However, domestic law has numerous safeguards in relation to right to private life and protection of personal data, and possible derogations from these rights. Constitution of republic of Serbia recognizes right to confidentiality of letters and other means of communication, and the derogation is possible "only for a specified period of time and based on decision of the court if necessary to conduct criminal proceedings or protect the safety of the Republic of Serbia, in a manner stipulated by the law".³⁶ In relation to right to protection of personal data "use of personal data for any the purpose other the one were collected for shall be prohibited and punishable in accordance with the law, unless this is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in a manner stipulated by the law".³⁷ Relevant laws are in accordance with this rights', for example investigation can be initiated against a specific person for whom there are grounds for suspicion that he/she has committed a criminal offence, or against an unknown perpetrator when there are grounds for suspicion that a criminal offence has been committed.³⁸ When it comes to the changes in the number of reported criminal offenses against sexual freedom at the beginning of pandemics, it seems that there are no significant changes in this respect (Đokić & Čvorović, 2014:270).

5. CONCLUSION

It seems that there is lack of timely and complete action of the Commission, in the matter that is recognized as a EU priority. Certainly, there was a focus on find-

³⁵ COM(2020) 607 final, p. 3.

³⁶ Official Gazette of the RS, No. 98/2006, Article 41.

³⁷ Official Gazette of the RS, No. 98/2006, Article 42.

³⁸ Official Gazette of the RS, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - decision CC and 62/2021 – decision CC, Article 295.

ing quick solutions to complex issues. It was convenient to find quick solution for growing online child sexual abuse in EU, and the extended scope of ePrivacy Directive just revealed privacy issues of the existing practice. Interference does not have firm legal basis. Also, respect of the essence of the right that is being restricted is questionable. There is no detailed analysis of necessity and proportionality of general processing of data in combating online child sexual abuse, and possible adverse effects on combating online child sexual abuse, especially whether this could make crime more difficult to detect in future, when offenders shift to other, less risky methods. This might lead to inclusion of other online crimes in general data scanning of private communications content. Ultimately, it must be considered why the privacy of online communications is less important than offline communication. If there is no difference, then this might lead to further privacy intrusions, as a legitimate method of fight against serious crimes. Some changes can be expected in close future, since there is a strong indication that the scanning will be mandatory for providers, but more importantly, end-to-end encrypted electronic communications might be included. Although, it must be admitted that the online privacy intrusions are aimed at “detecting patterns”, and not full access to content. In this respect, assessment of concrete technology reliability, for processing of certain forms of data is essential.

REFERENCES

1. Abelson H., Anderson R., et al. (2021), “Bugs in our Pockets: The Risks of Client-Side Scanning”, arXiv, Cornell University, 2021, pp 1-46., <https://doi.org/10.48550/arXiv.2110.07450>, accessed on 07. 04. 2022.
2. Baron R. M. F. (2002) A Critique of the International Cybercrime Treaty, *Journal of Communications Law and Technology Policy*, 10 (2), pp. 263-278.
3. Bertuzzi L. (2021), New EU law allows screening of online messages to detect child abuse, Euractiv, <https://www.euractiv.com/section/data-protection/news/new-eu-law-allows-screening-of-online-messages-to-detect-child-abuse/>, accessed on 06. 04. 2022.
4. Charter of Fundamental Rights of the European Union. Official Journal of the European Union. C 326/391, 26.10.2012.
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions EU strategy for a more effective fight against child sexual abuse, Brussels, 24.7.2020, COM(2020) 607 final.

6. Constitution of Republic of Serbia, Official Gazette of the RS, no. 98/2006.
7. Council of Europe (2021) Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse- Independent experts' report, Directorate General of Human Rights and Rule of Law - DG I and Directorate General of Democracy - DG II
8. Criminal Procedure Code, Official Gazette of the RS, no. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - decision CC and 62/2021 – decision CC.
9. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Official Journal of the European Union, L 321, 17.12.2018.
10. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance, Official Journal of the European Union, L 321, 17.12.2018.
11. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Union, L 201, 31.7.2002.
12. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal of the European Union, L 335, 17.12.2011.
13. Đokić I., Čvorović D. (2021) Criminal Legal Challenges in Republic of Serbia during COVID-19 Pandemic, *Crimen*, XII (3), pp. 259–276
14. EDPS (2020) Opinion on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, https://edps.europa.eu/sites/default/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf, accessed on 30. 03. 2022.
15. EDRI (2021) Wiretapping children's private communications: Four sets of fundamental rights problems for children (and everyone else), <https://edri.org/our-work/children-private-communications-csam-fundamental-rights-issues/>, accessed on: 02. 04. 2022.
16. EDRI (2022) Scanning private communications in the EU EDRI's principles for derogating from the ePrivacy Directive for the purpose of detecting online child sexual abuse material, <https://edri.org/wp-content/uploads/2022/02/EDRI-principles-on-CSAM-measures.pdf>, accessed on: 05. 04. 2022.

17. EPRS (2021) Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse – Targeted substitute impact assessment, Brussels.
18. Eurochild (2021) Eurochild calls on the EP to keep children safe online by adopting a Temporary Derogation to the ePrivacy Directive, <https://www.eurochild.org/news/eurochild-signs-joint-letter-asking-to-adopt-a-temporary-derogation-to-the-eprivacy-directive/>, accessed on 31.03. 2022.
19. European Commission (2021) Commissioner Johansson’s speech at the plenary debate on the use of technologies for data processing to fight online child sexual abuse, https://ec.europa.eu/commission/commissioners/2019-2024/johansson/announcements/commissioner-johanssons-speech-plenary-debate-use-technologies-data-processing-fight-online-child_en, accessed on 31.03. 2022.
20. European Data Protection Board (2020) Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 1.0, Adopted on 15 December 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf, accessed on 02. 04. 2022.
21. Explanatory Report to the Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185, Council of Europe.
22. Internet Watch Foundation (2020), The Annual Report 2020- Geographical hosting, <https://annualreport2020.iwf.org.uk/trends/international/geographic>, accessed on 31.03. 2022.
23. Interpol (2020) INTERPOL report highlights impact of COVID-19 on child sexual abuse, <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse>, accessed on 08. 04. 2022.
24. La Quadrature du Net and Others v Premier ministre and Others, Judgment of the Court (Grand Chamber) of 6 October 2020, ECLI:EU:C:2020:791.
25. Pia J., Bonnici M. (2014) Exploring the non-absolute nature of the right to data protection, *International Review of Law, Computers & Technology*, 28(2), pp. 131-143.
26. Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, Brussels, 10.9.2020, COM/2020/568 final.

27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119, 4.5.2016.
28. Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, Official Journal of the European Union, L 274/41, 30.7.2021.
29. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CM(2021)57-final, 17 November 2021.
30. US National Center for Missing and Exploited Children, Battle Won, But Not the War in the Global Fight For Child Safety, <https://www.missingkids.org/childsafetyfirst>, accessed on 29.03. 2022.
31. Wällgren M. (2016) Exploring the Outer Limits of Article 114 TFEU – towards a general power?, Master's Thesis, Uppsala Universitet.
32. WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children, UNESCO (2020) COVID-19 and its implications for protecting children online, <https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf>, accessed on: 02. 04. 2022.

BORBA PROTIV SEKSUALNOG ZLOSTAVLJANJA DECE NA INTERNETU U EVROPSKOJ UNIJI I OPŠTA OBRADA ELKTRONSKIH KOMUNIKACIJA³⁹

Borba protiv seksualnog zlostavljanja i seksualnog iskorišćavanja dece prepoznata je kao prioritet u okviru EU, s obzirom na zabeležen porast otkrivenih slučajeva seksualnog zlostavljanja putem interneta poslednjih godina. Da bi rešila pitanje seksualnog zlostavljanja dece na internetu, EU je pribegla dobrovoljnoj praksi obrade interpersonalnih elektronskih komunikacija od strane pružalaca usluga, koje nije zasnovano na čvrstoj pravnoj osnovi. Nakon proširenja obima Direktive 2002/58/EC o obradi ličnih podataka i zaštiti privatnosti u elektronskom komunikacionom sektoru, ova dobrovoljna praksa je privremeno obustavljena, do usvajanja Uredbe (EU) 2021/1232 o privremenom odstupanju od određenih odredbi Direktive 2002/58/EC. Međutim, čini se da predviđena ograničenja prava na privatnost i zaštitu podataka o ličnosti ne poštuju suštinu ovih prava, nije izvršena detaljna analiza neophodnosti i proporcionalnosti opšte i neselektivne obrade komunikacija svih korisnika, ali ni mogućih štetnih posledica na suzbijanje seksualnog zlostavljanja dece na internetu.

KLJUČNE REČI: seksualno zlostavljanje dece / privatni život / zaštita ličnih podataka / Uredba (EU) 2021/1232 / elektronske komunikacije

³⁹ Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)

CHILD PORNOGRAPHY ON THE INTERNET: CRIMINOLOGICAL ASPECT AND COMPARATIVE REGULATION

Aleksandar STEVANOVIĆ, MA¹

In order to contextualize the problem of child pornography, the author first strives to analyze the terms “pornography” and “child” in the context of the criminal law norm since it is imperative from a legal point of view to define what constitutes child pornography. Already at that step, many difficulties were pointed out, which are further implied on the adequate legal fight against child pornography. In the fight against child pornography. The influence of online technologies and Internet on the changed nature and phenomenology of child pornography was especially considered. We especially pointed out that although the Internet makes it easier for criminals to engage in activities that fall under child pornography, child pornography would not have become so visible without the Internet. Although the constitution of incrimination of child pornography is deeply determined by the cultural and social basis in general, it is necessary to establish harmonization in terms of the legal fight against child pornography in order for it to be effective. In this context, we have analyzed several legal definitions of child pornography in both universal and regional legal acts.

KEY WORDS: child / pornography / sexual abuse / internet / organised crime

¹ Research Associate, Institute of Criminological and Sociological Research in Belgrade, aleksandar.stevanovic993@gmail.com

1. INTRODUCTION

Modern society is largely determined by the use of technology that permeates human life in all fields. With the development of digital technologies, the broadcasting of various content, first on rare large cinema screens, and then on TV screens that were slowly “occupying” households, has become relatively easily accessible to a large number of people.

The abuse of various forms of social progress, such as technology, is a commonplace in the history of social community, and it has been particularly present in recent decades when it comes to the use of the Internet. Under the influence of the technological factor, the phenomenology of crime has been changed, so with the greater presence of high technology in everyday life, there has been a transformation of criminal opportunities and behavior. Criminal activities have become global, distributive and informationalized (Wall, 2015: 86). Crimes can be committed efficiently “remotely”, and the automation of technology contributes to the fact that an increasing number of potential perpetrators may abuse the opportunities it provides, with an increased chance of remaining undetected.

According to some sources, the presentation of pornographic content was first recorded a little over 600 years ago (Uljanov, Ivanović, 2009: 171). Due to its nature, erotic content is highly attractive to people, and despite the various restrictions that have been prescribed through different political and cultural phases of society, erotic content has spread easily, bringing on the one hand easy and quick earnings to the one who distribute it, and on the other hand easy pleasure for consumers.

Treating children as sexual objects is as old as humanity, and the history of creating erotic literature and drawings that include children is long. However, only recently, the dissemination of sexual materials on children depends on the technologies available for their creation and further distribution. The availability of cameras from the middle of the 19th century enabled the emergence of child pornography as we know it today (Mančević, 2016: 14). With the processes of digitalization and with the daily use of the Internet child pornography materials dissemination has become a relatively good criminal opportunity in terms of lucrativeness and difficulties in detecting crime. The advent of complex, and advanced technology offered internet users unparalleled anonymity and efficiency, giving offenders the means to share and sell child pornography materials through such networks while creating newer challenges of enforcement and policy response.²

² See: <https://www.cyberpeace.org/CyberPeace/Repository/End-to-end-Encrypted-CSAM-2.pdf>, date of access 7.5.2022.

However, until the mid-1990s, child pornography was not perceived as a particularly significant element in the array of activities related to sexual abuse. On the contrary, the dominant attitude was that it was a specific sexual deviation of a smaller scale compared to the pornographic content in which adults are portrayed (Taylor, Quayle, 2003: 1). However, after the mid-1990s, the problem gained in importance in both the professional and lay minds and is slowly becoming a topic of penal policy in many countries. According to some research, it is a multi-billion dollar industry nowadays.³ This state of affairs has caused increased normative activity, and from a time distance of several decades, we can already discuss about the quality of normative solutions that are current in different countries in terms of systemic fight against child pornography. Nevertheless, child pornography on the internet take place within a subculture that operates beyond the boundaries of any particular state or legal jurisdiction and represents a new pattern of globalized deviance (Jenkins, 2001: 5) and in an effort to gain insight into the etiology and phenomenology of the phenomenon, it is necessary to analyze it from a multidisciplinary point of view.

2. DEFINING NOTIONS ACCORDING TO CRIMINAL LAW RELEVANCE

The occurrence of sexual acts involving children is certainly not a new phenomenon and has existed in various forms throughout history. Child pornography is a form of child sexual exploitation in terms of visual depiction of sexually explicit conduct involving a minor. This is a serious sociological, criminological and victimological problem, the misuse and exploitation of computers and computer networks, most often the Internet, for the production, sale, exchange, possession and viewing of pornographic material in which the main actors are minors, in order to satisfy perverted sexual urges or gain material benefits (Mančević, 2016: 14).

In order to conceptualize the phenomenon of child pornography within the normative system of criminal law, definition difficulties must be overcome. First of all, when it comes to the legislation (criminal) where the concept of pornography is not precisely defined, it is necessary to determine it not only because of the understanding of the material content of the concept of pornography, but also because of procedural guarantees of criminal procedure, ie important criminal principles such as - *nulla poena sine lege stricta*. In light of such efforts it should be noted that pornography is a protean term determined by numerous cultural and

³ See: <https://globalinitiative.net/analysis/stolen-innocence-the-online-exploitation-of-children/>, date of access 5.5.2022.

social influences in general. Sometimes it is even very difficult to distinguish pornographic content from artistic expression. perhaps the best description of confusion and dependence on subjective experiences when it comes to defining pornography is summarized in quoted line from Supreme Court Justice Potter Stewart in 1964: “. . . I know it when I see it.” However, legal definitions tend to emphasize obscene or sexual content as an essential quality, but of course such definitions may vary depending on the legislature within a given country.

It seems that the definition according to which pornography is visual or written matter designed to cause sexual arousal⁴ is the most employed today. Consequently, useful definition has three components: content, the intention of the producer, and contextual judgement (Ashton et al. 2018: 150). Child pornography is for that reason defined in three stages: production, distribution and downloading of abusive material.

The ways that we define what it is to be a child are socially and temporally situated. Consistent with the UN Convention on the Rights of the Child, there is global trend towards an embracing view that childhood ends at 18 and persons under the age of 18 are commonly called juveniles. Most criminal justice systems distinguish between children under the age of 14 and those who have reached the age of 14 but not 18. In that sense, stricter sanctions are usually prescribed for criminal acts when the victims are children under 14 years.

Although in several domestic legal frameworks, the age of sexual consent is less than the minority age criteria, what is considered to be important for strengthening individual personality capacities, there is no relevance of consent when it comes to the child pornography. However, when viewing a picture consisting of pornographic content, attempting to determine an age may become a matter of complex judgement. Whilst decisions about whether a person photographed is a child are not problematic when the individual is very young, moving into adolescent years such decisions, when based on visual evidence, are much more difficult to make (Taylor, Quayle, 2003: 1). Simply put, an individual could enter a criminal zone by accident, while on the other hand he could escape if it turns out that the picture shows a person older than 18. Such a difficulty could be avoided with adequate norming. For instance, in the case when child pornography in terms of content is, among other things, defined as pornographic material that visually depicts a person appearing to be a minor.

At the international and regional level, there are various legal instruments/definitions that deal with child pornography. When it comes to the legalistic defini-

⁴ See: <https://www.merriam-webster.com/dictionary/pornography#note-1>, date of access 5.5.2022.

tions, the European Union's Framework Decision on combating the sexual exploitation of children and child pornography,⁵ which entered into force in January 2004, defines child pornography in article 1(b) as pornographic material that visually depicts or represents: (i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or (iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i).

The Council of Europe's Cybercrime Convention 2001,⁶ which came into force on 1 July 2004, defines child pornography, under article 9(2), as pornographic material that visually depicts: (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; (c) realistic images representing a minor engaged in sexually explicit conduct.

As for the U.S. legislation, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography,⁷ which came into force on 18 January 2002, defines child pornography in article 2(c) as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

3. CHILD PORNOGRAPHY AND INTERNET

Almost 54 percent of the world's population (4.1 billion people) uses the internet. It's our source of instant information, entertainment, news, and social interactions.⁸ As it is stated previously, child pornography has emerged as a global threat under the the rapid technological advancement facilitating easy and cheaper internet access, a massive increase in number of smart phones users, a boom of

⁵ Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004F0068>, date of access 5.5.2022.

⁶ Convention on Cybercrime, ETS No. 185, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>, date of access 5.5.2022.

⁷ Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, <https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child>, date of access 5.5.2022.

⁸ See: <https://globalfreedomofexpression.columbia.edu/publications/?f-search=censorship>, date of access 5.5.2022.

social media, end to end encryption and cloud based services (report). All these circumstances have opened some questions regarding the content of the incrimination in question. For example, technology is now allowing the creation of lifelike child pornography without the use of children at all (Healy, 1997). The question therefore arises about whether production, distribution or use of pseudo-photographs or computer generated images, drawings, cartoons and paintings is incriminated. Many national legislations leave this question open, but it seems that the answer has been given at the universal and regional level, according to which the enumerated online imaginations of children in the sexual context enter the zone of incrimination. The Explanatory Memorandum of the Council of Europe's Cyber-crime Convention 2001 states that 'it is widely believed that such material and online practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.' (Akdeniz, 2016: 11).

Although criminal jurisdiction is conceived according to the borders of the state, it has long been clear that online crime exceeds that limit, what poses major problems for law enforcement agencies in the application of both material and procedural norms. Real enforcement action must require co-operation amongst agencies in multiple jurisdictions which becomes difficult and complicated when a local agency undertakes an investigation. Despite that, it seems that the problem of child pornography would not have become so visible without the Internet. The problem became more prominent in the 1990s, however, with the widespread use of the Internet (Akdeniz, 2016: 6). In the past, obtaining child pornography was difficult since it required a measure of physical exposure of the person involved to being identified, in that a visit to a specialised sex shop was required, or a name and address had to be given to a mail order organisation. The private exchange of pictures between individuals also took place, but again the danger of identification remained (Taylor, Quayle, 2003: 1). Nowadays, in many cases, law enforcement agencies have located perpetrators of child pornography online using sophisticated online knowledge. For instance, global platform ICSE used by Interpol enables specialist officers to use sophisticated database comparison software in order to make connections between victims, abuser and locations.⁹

Child pornography material proliferation on the Internet is found under three heads based on the search-ability of content by standard web search engines, namely (i) Surface Web or Public Internet which is readily available to the general public. ; (ii) Deep web, which is not indexed by standard search engines and requires

⁹ See: <https://www.interpol.int/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims>, date of access 5.5.2022.

knowledge of direct URLs, IP addresses, credentials etc. to access, (iii) Dark web. While the dark web is still an evolving space on the internet, it is largely understood as the space which requires specialised software in order to be accessed.¹⁰

Table 1 below shows the most popular and widely used communication services:

Service	Global user base	E2EE in personal chats	E2EE in group/channel	Group/ channel invites through link
Facebook Messenger	1.3 billion	Optional, needs to be enabled for specific chats	No	No
WhatsApp	2 billion	Yes	Yes	Yes
Viber	1.17 billion	Yes	Yes	Yes
iMessage	Statistics not available publicly	Yes	Yes	No
Telegram	400 million	Yes, only in secret chats	No	Yes

Source: Report, *End (-to-end encrypted) Child Sexual Abuse Material*, 2020 Cyber Peace Foundation¹¹

It could be safely concluded that the biggest problem in detecting child pornography arises when it takes place within the Dark Web. On the other hand, although the business on the Internet is still insufficiently precisely regulated, technical possibilities provide various solutions for the fight against child pornography, which are recognized and applied by certain legal systems. Of course, this is possible when certain measure needs to be taken against legal entities that are registered in accordance with the law, such as *Facebook*, *TikTok*, etc. For instance, the Italian Data Protection Supervisory Authority issued two interim measures restricting the ability of social media platform, *TikTok*, from processing the data of users residing in Italy whose age could not be determined by certainty. It was stated that, although *TikTok* had a policy of denying access to its platform for children who are younger than 13 years old, this could be easily circumvented as the age verification procedure relied on the user’s self-declaration.¹²

¹⁰ See: <https://www.cyberpeace.org/CyberPeace/Repository/End-to-end-Encrypted-CSAM-2.pdf>, date of access 7.5.2022.

¹¹ *Ibidem*

¹² See: <https://globalfreedomofexpression.columbia.edu/cases/italian-data-protection-authority-v-tiktok/>, date of access 7.5.2022.

Attempts to control child pornography on the Internet have brought into focus critical issues related to the nature of the Internet as a medium of information transmission, and the social context in which that information is transmitted. A central issue for policy makers is the problem of reconciling *freedom of speech* and limitations on censorship of the Internet with the very evident child-protection problems presented by the production, distribution and viewing of child pornography (Taylor, Quayle, 2003: 1).

In one case from U.S. case law (U.S., *State v. Packingham*, 777 S.E.2d 738 (N.C. 2015) the court found a violation of the plaintiff's rights due to the fact that the law that regulated access to Internet content for registered sex offenders did so in an overly broad and not narrowly tailored way. Namely, the Supreme Court of the United States found a law in North Carolina to be in violation of the First Amendment because it made it a felony for a registered sex offender "to access a commercial social networking Web site where the sex offender knows that the site permits minor children to become members or to create or maintain personal Web pages." The case was taken by a registered sex offender who had been convicted under the law after publishing a *Facebook* post in 2010. The Supreme Court of the United States reached its decision because the law was overly broad and not narrowly tailored to further the government's legitimate interest in preventing child abuse. They went on to state that cyberspace had become the most important place for the exchange of views and in light of the constantly developing nature of the Internet, the Court concluded that it "must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks."¹³

It is generally accepted attitude that whilst it is important to create an environment in which children are not abused, it is also necessary to recognize the limits that protection can take (Taylor, Quayle, 2003: 8).

4. PHENOMENOLOGICAL CHARACTERISTICS OF CHILD PORNOGRAPHY

It seems that the Internet has greatly contributed to the change in the phenomenology of many crimes, which is also the case when it comes to child pornography. According to Global Initiative Against Transnational Organised Crime two trends have emerged in online child sexual exploitation in recent years.

¹³ See: <https://globalfreedomofexpression.columbia.edu/cases/packingham-v-state-north-carolina/>, date of access 7.5.2022.

Firstly, the increasing prevalence of home-produced abusive material as well as live video streaming of children being forced to perform sexual acts in front of a webcam. This rapidly growing new form of child pornography allows the user to direct and make online requests for particular sexual activities to be carried out on the victim in real time. Secondly, predators are taking sophisticated security measures to share files directly between users instead of downloading them from a website. P2P is most frequently used for sharing images of very young children or of images portraying violence against children.¹⁴

In general, the incrimination of child pornography is not easy to classify and typify, since its predominant characteristics include the basic elements of different criminological classifications. Furthermore, the range of people involved in child pornography offences seems to cross boundaries of class, income and profession. Doctors, technicians, businessmen, teachers, media personalities, policemen: these are just a few of the kinds of people who have been found guilty in recent criminal proceedings of possession of child pornography (Taylor, Quayle, 2003: 7).

Activities that fall under child pornography can be performed as profit or non-profit motivated. Child Protection Act of 1984, made significant changes in comparative legislation, by removing the requirement that the transmission or receipt of child pornography be done for profit, thereby targeting the growing non-commercial cottage industry (Adler, 2001: 39). Today, it is generally accepted attitude that activities that fall under child pornography can be performed as profit or non-profit motivated.

In the context of profit driven child pornography, it is important to point out that it is the subject of activities of many organized criminal groups that operate transnationally. Organized crime operates in areas where there is money and opportunities for easy and large profits. As Serious and Organised Crime Agency UK (SOCA) warned more than 15 years ago, organised criminals are massively moving into child pornography business.¹⁵ Carrying out criminal activity on the Internet enables easy creation of a criminal network and its establishment without a lot of invested resources. Also, the Internet provides the possibility for criminal groups to be present in any market with only 'one click. For these reasons, even more extensive activities related to child pornography by organized criminal groups can be expected.

¹⁴ See: <https://globalinitiative.net/analysis/stolen-innocence-the-online-exploitation-of-children/>, date of access 5.5.2022.

¹⁵ See: <https://www.theguardian.com/uk/2006/jul/31/immigration.ukcrime>, date of access 5.5.2022.

Two important criminological phenomena are related to child pornography. Firstly, when it comes to child pornography, as a rule, there has been growing panic in recent decades. In this regard, the consequence is often an uncritical view of the problem while indulging in criminal populism, which often results in inadequate and inapplicable legal responses.

Secondly, as we discussed earlier, the Internet is a platform on which activities that fall under child pornography are most often performed is still an unregulated zone. This further means that there is a large dark figure of crime when it comes to child pornography which is important to take into account when researching this problem and designing legal and non-legal mechanisms to combat child pornography.

5. CONCLUSION

Until recently, child pornography was rarely identified as a factor in child sexual abuse, not necessarily because taking sexual photographs of children did not occur, but because, in the main, social welfare intervention with survivors of child sexual abuse has not seen it as a particularly relevant factor in treatment or counselling. However, accelerated digitization and development of the Internet has drawn our attention to the existence of child pornography in a very dramatic way. Things became even more complex when organized crime became massively involved in the business of child pornography on the Internet. However, regardless of the fact that the Internet makes it easier for criminals to engage in activities that fall under child pornography, it should be noted that child pornography would not have become so visible without the Internet.

From the aspect of protection of human rights, especially freedom of speech, there are certain problems regarding censorship and free access to information on the web, but however The laws on Child Pornography is the least controversial area of jurisprudence of the First Amendment, and the same could be said when it comes to the cases of the European Court of Human Rights.

Child pornography law is a remarkably recent invention and there is still a lot of space to improve legal response to the child pornography in terms of international harmonization which is necessary precondition for fight against child pornography since Internet profligation transcending the boundaries of national jurisdictions. In light of this, a good starting point for harmonizing national jurisdictions could be European Union's Framework Decision on combating the sexual exploitation of children and child pornography, The Council of Eu-

ropé's Cybercrime Convention 2001 or Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography in U.S since The listed legal acts recognize all contemporary difficulties in defining and combating child pornography, which are most often the result of cultural and technological circumstances, and with their adequate nomotechnics offer legal mechanisms for overcoming these difficulties.

REFERENCES

1. Adler, A. (2001) The Perverse Law of Child Pornography. *Columbia Law Review* 101.
2. Akdeniz, Y. (2016) *Internet child pornography and the law: national and international responses*. London: Routledge.
3. Ashton, S., McDonald, K., Kirkman K. (2019) What does 'pornography' mean in the digital age? Revisiting a definition for social science researchers. *Porn Studies*, vol. 6 iss. 2.
4. Healy, M. (1997) Child pornography: An international perspective. Prepared as a working document for the World Congress Against Commercial Sexual Exploitation of Children in 1997.
5. Jenkins, P. (2001) *Beyond Tolerance: Child Pornography on the Internet*, New York: New York University Press.
6. Mančević, M. (2016) *Dečija pornografija kao oblik visokotehnološkog kriminaliteta*. Pravni fakultet u Nišu.
7. Taylor, M., Quayle, E. (2003) *Child Pornography: An Internet Crime*. Hove: Brunner Routledge.
8. Uljanov, S., Ivanović, Z. (2009) Seksualna eksploatacija dece sa aspekta uporednopravne analize međunarodne saradnje u kriminalističkim istragama. *Evropsko zakonodavstvo*, br. 29-30.
9. Wall, D. (2015) Dis-organised crime – towards a distributed model of the organization of cybercrime. *European Journal of Organised Crime* no2.

Interent sources

1. Convention on Cybercrime, ETS No. 185, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>
2. Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004F0068>

3. <https://globalfreedomofexpression.columbia.edu/cases/italian-data-protection-authority-v-tiktok/>
4. <https://globalfreedomofexpression.columbia.edu/cases/packingham-v-state-north-carolina/>
5. <https://globalfreedomofexpression.columbia.edu/publications/?f-search=censorship>
6. <https://globalinitiative.net/analysis/stolen-innocence-the-online-exploitation-of-children/>
7. <https://www.cyberpeace.org/CyberPeace/Repository/End-to-end-Encrypted-CSAM-2.pdf>
8. <https://www.interpol.int/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims>
9. <https://www.merriam-webster.com/dictionary/pornography#note-1>
10. <https://www.theguardian.com/uk/2006/jul/31/immigration.ukcrime>,
11. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, <https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child>

DEČIJA PORNOGRAFIJA NA INTERNETU: KRIMINOLOŠKI ASPEKT I UPOREDNOPRAVNA ANALIZA¹⁶

U cilju kontekstualizacije problema dečije pornografije, autor je najpre nastojao da analizira pojmove “pornografije” i “deteta” u kontekstu krivičnopravnih instituta i zakonodavstva uopšte. Već na tom prvom koraku, ukazano je na brojne poteškoće koje se dalje efektuju na odgovarajuću pravnu borbu protiv dječije pornografije, a koje su u osnovi posledica kulturoloških okvira, ali i procesa digitalizacije i “internetizacije” sadržaja u modernom društvu. Posebno je razmatran uticaj online tehnologija i interneta na izmenjenu prirodu i fenomenologiju aktivnosti koje potpadaju pod krivičnopravni pojam dečije pornografije. U radu je naglašena činjenica da iako internet olakšava bavljenje aktivnostima koje spadaju u dečiju pornografiju, ona sa druge strane ne bi postala vidljiva oku javnosti i ne bi bila percipirana kao krupan izazov za kaznenu rekaciju bez uticaja interneta. Iako je konstituisanje inkriminacije dečje pornografije duboko determinisano kulturološkim i društvenim osnovama uopšte, neophodno je uspostaviti harmonizaciju u pogledu pravne borbe kako bi ona bila delotvorna. U tom kontekstu, analizirali smo nekoliko zakonskih definicija predmetnog pojma kako u univerzalnim tako i u regionalnim pravnim dokumentima.

KLJUČNE REČI: deca, pornografija, seksualna zloupotreba, internet, organizovani kriminal

¹⁶ Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)

TECHNOLOGY-ASSISTED CHILD SEXUAL ABUSE, EXPLOITATION AND TRAFFICKING¹

Jasna HRNČIĆ, PhD²

Nina LONČAR, PhD³

Child sexual abuse (CSA) is one of the most devastating forms of human communication. In the last decades it is facilitated by information communication technologies (ICT). The authors analyse characteristics and specifics of ICT-assisted child sexual abuse, including exploitation and trafficking of children in order to provide better understanding of the phenomenon. Terms in the field have been examined, online environments as a risk factor analysed, prevalence of the phenomenon presented. Motivation, implicit theories and cognitive distortions of offenders are explained. Current typologies of ICT assisted CSA offences and offenders and risk factor for victimization are inspected. The differences and overlaps between terms and typologies in the field are discussed and barriers to effective prevention and intervention analysed. Urgency for effective social reaction to this blatant evil is emphasized.

KEY WORDS: Internet / child sexual abuse / child sexual exploitation / child sex trafficking / typology / risk factors.

1. INTRODUCTION

Continuous evolution of information communication technologies (ICT) have been transforming children lives in many ways. American teens report that 95%

¹ The contribution of Jasna Hrnčić to the paper was financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia as a part of the Plan for Scientific Research of the University of Belgrade - Faculty of Political Science.

² Full Professor, Faculty of Political Science, University of Belgrade, jhrncic@gmail.com

³ JU Retirement Home "Pljevlja", Montenegro, ninaloncar111@gmail.com

of them have access to smartphone and 45% of teens are online almost constantly (Anderson & Jiang, 2018). Researches conducted in our region in 2016, thus before on-line schooling, showed that 97% high school students in Serbia (Kuzmanovic, 2016) and primary school students in Montenegro (Hrncic & Loncar, 2016:5) was using internet, while 99% of Serbian student (Kuzmanovic, 2016) and 68% of Montenegrin students had smartphone (Hrncic & Loncar, 2016:5). The study in Montenegro found that also almost half pupils were on internet 3 or more hours. The internet is mostly used for schoolwork, online games, film clips and social exchange (Medierådet, 2017). It is used to initiate, maintain and expand communication for friendship, love and/or sex. In parallel unpleasant, hostile, abusive and exploitative exchanges have been multiplied through ICT thus creating online content that is often disturbing and sometimes illegal (Quayle, 2017). One of the most harmful exchanges would be child sexual abuse (CSA) in a broad span from unwanted sexual approaches to a rape documented, shared and sold by ICT technologies as a newly aggravated crime with especially devastating consequences. ICT facilitate CSA through anonymity of both users and traffickers, affordable prices for the services of ICT, low cost accessibility of CSA to users, lucrative trade through internet that require little investments and lack of appropriate legislation to fight the phenomena (Council of Europe, 2003). Consequences for the victim depends on gravity of CSA and could encompass lower self-esteem, distrust in sexual encounters and withdrawal from on line communication for CSA of lower intensity, through disturbed sexual development and partnership in more serious cases, to mental disorders (depression, PTSP, anxiety, dependence from psychoactive substances – PAS, Stockholm syndrome and antisocial behaviour), as well as physical injuries and diseases that could lead to early death as it is the case with victims of child sex trafficking (CST).

This study aims to analyse characteristics and specifics of ICT-assisted child sexual abuse, including exploitation and trafficking of children in order to provide better understanding of the phenomenon.

2. DEFINITIONS

Several terms are frequently in a use in the area, and most of them are overlapping in everyday practice. Child sexual abuse (CSA) is defined by Council of Europe as a crime and includes: (a) “engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities” (does not apply to consensual sexual activities between minors), and (b) “engaging in sexual activities with a child by coercion, force or threats; or

by abuse of a recognized position of trust, authority or influence over the child, including within the family; or abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or situation of dependence” (Council of Europe, 2007, article 18.1 and 18.3). Child is defined as “any person under the age of 18” (Council of Europe, 2007, article 3).

Child sexual abuse becomes sexual exploitation when a second party have material benefits from sexual activity involving a child. It includes child pornography and child prostitution. Child pornography means “...any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes” (Council of Europe, 2007, article 20.2). Child prostitution means “...the using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person (Council of Europe, 2007, article 19.2). Severe form of sexual exploitation is the sex trafficking as “...the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act” (U.S. Department of State, 2000, sec.103.9). It is also called modern days slavery. Severe form of human trafficking is “...sex trafficking in which the person induced to perform commercial sex act has not attained 18 years of age”, regardless of the “use of force, fraud, or coercion” (U.S. Department of State, 2000, sec.103.8).

Technology-assisted child sexual abuse (TA-CSA, Hamilton-Giachritsis et al., 2018:5) could be defined as at least partly facilitated by ICT, that is the internet or other wireless communications (Committee on the Rights of the Child, 2019). Term “Internet offending” describe a range of Internet facilitated offenses (Taylor & Quayle, 2010:81) while “Internet crimes against children” are defined as offenses that include elements of computer facilitated sexual exploitation of minors (Alexy et al., 2005:804).

2.1. Online environments as a risk factor for CSA

Human interactions on the Internet are still evolving and are not completely understood. Especially rapid is production of new applications for smartphones and its use in daily life.

The Internet use of children is more intensive, extensive and skilled than that of adults (Parti & Virag, 2012:72). It is justified to say that “...parents are digital immigrants in the world of digital native children” (Prensky, 2007:2). Children behaviour online is therefore often unsupervised and they are online almost constantly. Frequent notifications, immediate access to information and social feedback aggravate the moderation of ICT use. More than 33% of smart phone users report

that they access their smart phones within the first five minutes of waking up and more than 40% check their phone during the night (Wigginton, Curran, Brodeur, 2017). Studies have shown association between excessive smartphone use and impulsivity (Schulz van Endert & Mohr, 2020:4) that is a risk factors of antisocial behaviour (Hrncic, 2009).

Young people frequently use social media sites, that are designed to encourage the sharing of information. Excessive and unconcerned use of ICT provide additional routes to access children and young people to abuse. A survey of 832 American teenagers found that a few teens embrace a fully public approach to social media yet only 9% of them state are “very” concerned about third-party access to their data (Madden et al., 2013). In comparison to result of the study on the same group in 2006, 91% post a photo of themselves up from 79% in 2006; 71% post their school name up from 49%, 71% post the city or town where they live up from 61%, 53% post their email address up from 29%, and even 20% post their cell phone number up from 2% (ibidem).

ICT often assist in initiation, maintenance and escalation of CSA. They increase an accessibility of victims, lower inhibitions, create feeling of powerlessness, increase use of the night time space, increase emotional and image related blackmail, reduce recognition of abuse and protection of victim and lower risk for detecting perpetrator. Internet also allowed for new modes of CSA to emerge, such as recording and uploading or live streaming of sexual assault, extortion or rape of children.

Heirman and Walrave (2008:5) identified most significant features of online communication in cyberbullying that facilitate online child sexual abuse: anonymity, the furtive nature of online communication, attainability, the absence of nonverbal cues and quick distribution of electronic messages to infinite audience.

Anonymity of online CSA shields the identity of perpetrators. Sometimes it is hard to distinguish even if the perpetrator is one individual or more of them. High protection of online identity has been acquired by the Dark Web⁴. Previously recorded rise of CSA in the Dark Web, where identities of perpetrators are hidden and identities children whose bodies are exposed in sexualized manner are often unknown has been accelerated since the outbreak of COVID-19 (Europol, 2014,

⁴ The dark web is the World Wide Web content that exists on *darknets*: overlay networks that use the Internet but require specific software, configurations, or authorization to access. Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location (Wikipedia, available at https://en.wikipedia.org/wiki/Dark_web, accessed on 27th April 2022).

2016, 2020). Internet Bulletin Board Systems enables images to be are uploaded to servers under a specific newsgroup heading, making them available to other users of that newsgroup worldwide (Beech et al 2008:221). A user can also share files on their computer using secure Windows' FTP server that allows other web users direct access to specified areas of a user's computer. Images can be exchanged privately between individuals using Internet Relay Chat (IRC) which allows its user to make data on their computer available to other IRC users. Images can also be exchanged privately through the direct exchange of e-mails (ibidem).

Large/infinite audience. Some areas of the Internet became platforms for child sexual abusers networking. Within seven forums dedicated to CSA on Dark Web there were more than two million unique user IDs (Web-Iq, 2018). Some groups have an entry requirement that locks its members into protecting each other, for example members had to submit 10,000 child pornography images (Krone, 2004:5).

The 24/7-attainability. Personalised mobile technology of smartphones enables users to bring their social networks wherever they go. As personal experiences have been connected and shared boundaries between the private and public sphere is blurred while time and place restrictions no longer exist. It victimizes children in more devastating way than ever before. For example, live streaming of CSA involves broadcasting that acts live via webcam to people anywhere in the world (ECPAT International 2017) while most videoclips could be reviewed at any time.

Private nature of online communication. While this is a chance for children to explore world of adults without their supervision, it also facilitates finding a vulnerable child, gaining his/her trust and grooming it for CSA.

The absence of non-verbal communication cues. In many online environments people cannot see each other and if they can ICT strips away many non-verbal cues, such as body language and voice fluctuations. It has a 'disinhibition effect' (Suler, 2004:3), allowing users to do things that they otherwise wouldn't.

The most popular vehicles for CSA are apps. The use of applications for mobile technology such as Snapchat, Frankly, Wickr, Blink and Glimpse "provide a social landscape through which teens survey themselves and others" (Charteris et al. 2014:2). In these applications images are automatically deleted shortly after being received enabling users to evade detection (ibidem). It is difficult to keep track of the apps since new apps continue to be released and online predators are among the first to sign up. San Diego County Human Trafficking Task Force suggested list of apps that predators frequently use and that are popular among children and adolescents: social media apps Live me, ASK FM, Holla, Whisper; dating apps like

Grinder, Skout,Badou, Plenty of fish, Meet me; messaging apps like Kik Calculator% (Hargrove & Avitabile, 2020).

Durkin (2018:4) identified a few most important ways in which Internet is used to sexually abuse children: 1) It is now the main mechanism to access and distribute child pornography. 2) It is used to facilitate the commercial sexual exploitation of children (child sex pornography and trafficking). 3) The Internet use as a social consolidation mechanism allowing adults with sexual interest in children to network with each other. 4) The Internet has secondary role in victimization of children allowing offenders to have preexisting relationship with minors to use it as a medium to facilitate contact offending.

3. TYPES OF OFFENCES

Although CSA could have low intensity like unwanted sexual approaches, most of technology-assisted CSA acts are offences. Hamilton-Giachritsis et al. (2018:12) differentiated several types of offences that could be summarised in following categories: 1) Sexual images created consensually but shared non-consensually. It implies the distribution of sexually explicit images or videos of individuals without their consent. 2) Technology assisted sexual blackmail. It could be use of child images abused offline as leverage in the continuation of the abuse, or use of child sexual images obtained via ICT as leverage in offline or/and technology assisted child sexual abuse. 3) Technology assisted grooming⁵. Perpetrators would forge a close relationship with a victim via ICT to gain the child's compliance in and secrecy around subsequent CSA. 4) Offline child sexual abuse shared with and viewed by others via technology. Abuse perpetrated by adults would be most frequently shared globally while abuse perpetrated by peers would probably be shared with the victim's peer group. 5) Offline contact CSA commissioned via technology. Purchaser use technology to witness (most usually watch) and direct child sexual abuse committed by other perpetrators who are physically with the child. 6) Sexual activity bought from a child advertising sexual services online for payment. The most usually the child has been previously severely abused.

This classification doesn't take into account CST practices, such as offline child sexual abuse sold to others via ICT, offline contact CSA bought from a trafficker advertising sexual services online, and other trafficking logistics including recruitment, organizing transport and networking via ICT. ICT could be used to recruit children for sex trafficking on social networks, to neutralize the law trough geo-

⁵ Grooming is a process by which a person prepares a child, significant adults and the environment for the abuse of the child (Craven et al., 2006:8).

graphical location of the server in the country where the legislation for technology assisted trafficking is weak or missing, to coordinate activities of organized sex trafficking, to advertise, sell, document and share sexual act over a child (Council of Europe, 2003).. Web pages and sites may contain advertisement for CSA and sex tours, information on how and where to find children to be bought for sex act, chat rooms for sexual exploitation of children (ibidem).

4. PREVALENCE OF CHILD SEXUAL ABUSE

Online CSA has been widely spread. Survey conducted on a national representative sample of 6,787 Swiss students with an average age of 15.5 years found that 40.2% of girls and 17.2% of boys reported having experienced at least one type of CSA event (Mohler-Kuo et al., 2014:306). The most frequently experienced is peer sexual harassment via Internet. More than 50% of female and 70% of male victims reported having been abused by juvenile perpetrators.

Research of unwanted sexual solicitations⁶ (USS) was conducted at three time points (2000, 2005, 2010) with separate US national samples of 1,500 internet users aged 10-17 and their parents (YISS, Mitchell et al., 2012:2). It indicated that USS was highest among children aged 10-12. It declined by 53% over the decade, from 19% in 2000 to 9% in 2010, while the proportion of aggressive USS (involving offline contact by the perpetrator through surface mail, telephone or in person, or attempts or requests for it) increased from 15% in 2000 to 34% in 2010. Aggressive USS included in 65% cases a request for sexual pictures of the child in 2010 (Mitchell et al., 2014).

That image dissemination of sexually abused children and adolescent is wide spread practice implicate finding that 250,000 American computers shared 120,148 child pornography images during a one year period (Wolak, Libertore & Levine, 2014:6). The COPINE database contained over 700,000 abusive images and noted many more images may still be held in private collections by May 2004 (Quayle, 2008:7). Between 2000 and 2006 year the number of arrests made for technology-facilitated sexual crimes against children in U.S. has been almost tripled (2,577 to 7,010) with a half of the arrests for the “possession of child pornography (Mitchel et al. 2014). Proportion of the offenders known to the victims has been increased two and a half times from 2000 to 2009 (ibidem).

Bissias et al. (2015) found about 840,000 installations per month on five popu-

⁶ Sexual solicitation is an unwanted sexual request by an adult (Kimberly, J.M., Finkelhor, D., Wolak, J., 2001:3011).

lar peer to peer (P2P) programs sharing child sexual exploitation material (CSEM) worldwide during a period of four years (2011-2014). They estimate that about 3 in 10,000 Internet users worldwide were sharing CSEM in a month. Every tenth (9.5%) person arrested for P2P-based CSEM trafficking on the studied networks was also identified as offline sex offender against children.

It is estimated that “at least 700,000 persons annually, primarily women and children, are trafficked within or across international borders. Approximately 50,000 women and children are trafficked into the United States each year” (U.S. Department of State, 2000, sec. 102.b), many of them “are trafficked into the international sex trade, often by force, fraud, or coercion.” (ibidem). There is significant increase in CST cases in U.S. from 97 cases in 2010 to 360 cases in 2015 (Roe-Sepowitz et al., 2017). International Organization of Migration (IOM) estimates that there are 700,000 victims of human trafficking per year from Eastern Europe former Soviet Union, Asia, Africa and Latin America (IOM, cited by Tan et al., 2014). Having in mind that 67.0% of sex trafficking survivors in U.S. in 2019 were under age of 18 at the time trafficking began and that the most probable age of recruitment of sex trafficking victims is between 12 and 17 (Statista, 2020), it becomes clear that victims of sex trafficking are mostly children. Data shows that 10% of CST survivors in U.S. in 2019 were children aged from 0 to 8 years (ibidem). Bunzeluk (2009) found that when CSA images included violent and/or extreme assault (e.g., torture, degradation, bestiality) victimized children were most likely to be under the age of eight.

5. CHARACTERISTICS OF OFFENDERS

Motivation, implicit theories and cognitive distortions of offenders

Curtis et al. (2013) proposed that consuming child sexual exploitation material (CSEM) is based on four motivations: (1) a specific sexual interest in children, (2) a general deviant sexual interest, (3) commercial motivation, or (4) other, like collecting of CSEM.

Ward and Kennon (1999) conceptualized one of the most prominent models that distinguish five implicit theories child sex offender have about the offence and victims: 1) *Children are sexual objects. Beliefs are: children able to have sexual feelings, enjoy and desire sex; expression of these desires is even beneficial. Typical cognitive distortion is: “Children often initiate sex and know what they want”.* 2) *Entitlement. Beliefs are that some people, and especially offender, are more important than others and thus they are above binding moral rules and have right to fulfil their needs. Typical cognitive distortion is: “Children are supposed to do what I want and*

serve me.” 3) *Dangerous world*. Basic believe is: “Beliefs and desires of other people threaten me.” It has two variations: a) “It is necessary to achieve dominance to survive, including women and children who threaten me”, with typical distortion: “I had to teach her a lesson”; and b) “Adults are unreliable, children are dependable, therefore children are only “safe” sexual partners.” Typical distortion is: “Children are innocent and want to please.” 4) *Uncontrollability*. Belief is that factors beyond control of the offender determine child sexual abuse. Typical cognitive distortions are: “I was in trance/drugged/drunk and it just happened.” 5) *Nature of harm*. Beliefs are: “Sexual conduct is beneficial by itself and unlikely to inflict harm. There are degrees of harm. If the injury could be more harmful the lesser act is more acceptable therefore offender is less guilty.” Typical distortions are: “It is acceptable for I didn’t use physical force”, “She is too young to understand and remember (abuse).” These implicit theories give basis to misinterpretation of a child behaviour and permission to CSA.

Paquette and Cortoni (2020) found two themes specific for online CSA: 1) *Virtual is not real*, stated by almost all CSEM offenders (CSEMOs) and offenders that solicitate children for sex (CSSOs); and 2) *Internet is uncontrollable*, supported by almost half of participants from both groups.

5.1. Types of offenders

Different typologies of online child sexual offenders help to grasp the phenomenon. Krone (2004) defined three behavioural factors that determine seriousness of CSA: 1) the nature of the abuse, from indirect to direct victimization; (2) the level of networking offender is a part of; and (3) the level of security offender employ to avoid detection. Based on these factors he classified involvement into CSA into several types: 1) Browser comes across child pornography unintentionally but saves it. 2) Private fantasy includes creation of online text of digital images for private use. 3) Trawler uses openly available networks to seek child sexual material. 4) Non secure collector downloads or exchanges child pornography mostly from openly available per-to-peer. 4) Secure collector uses security barriers to collect pornography. 5) Online groomer initiates online contact with a child with the intention to establishing a sexual relationship involving cyber-sex or physical sex. 6) Physical abuser actively abuses the child and may or may not use child pornography. 7) Producer record CSA committed by himself or by other offenders. 8) Distributor of any of above activities may or may not have a sexual interest in child pornography.

Most offenders apply low level of security measures. Wolak, Finkelhor, and Mitchell (2005) found that only 20% of survey participants used sophisticated measures to hide images on their computer, such as: password protection (17%),

encryption (6%), file servers (4%), evidence-eliminating software (3%), remote storage systems (2%), and partitioned drives (2%). Similarly, Carr (2004) found that 75% of their sample had taken no security measures to protect their collection and only a small number of offenders had applied a password system (8%), encrypted their data (6%), or even saved the data to an ambiguously named folder (6%). High level security measures are connected to more serious offences as contact CSA and trafficking.

Hartman et al. (1984:5) differentiated four types of collectors of images of CSA: 1) Closet type hides their collections and evades contact CSA. 2) Isolated type both collects abusive images and have contact CSA. 3) Cottage type shares their collection with the others of the kind mostly for verification. 4) Commercial collectors exploit their collection for financial gain.

Alexy et al. (2005) defined three behavioural types of offenders: traders, who traffic and collect abusive images of children online (non-contact offenders), travellers that use the Internet to coerce and manipulate children into contact CSA, and trader-travellers that combine characteristics of the two types simultaneously.

Beech et al. (2008:225) categorised Internet offenders into four groups: (1) individuals who access images of CSA sporadically, impulsively and/or out of curiosity; (2) those who access/trade images of CSA to charge their sexual interest in children; (3) persons who's Internet use is a part of a schema of offline contact CSA, including (i) those who online locate/groom contact victims and (ii) those who disseminate online images of CSA they have produced; and (4) individuals who access images of CSA for seemingly non-sexual reasons like financial profit.

All above typologies differentiate *between those who engage in CSA primarily for personal pleasure (consumers) and those who use CSA primarily for commercial purposes (commercial collectors and traffickers)*. Most of typologies also distinguish *between internet use to access and share child abusive images (non-contact or indirect offenders) and to enable contact (or direct) offending* (Krone, 2004, Alexy et al., 2005, Kettleborough & Merdin, 2017, Brown & Bricknell, 2018), *with overlapping between non-contact and contact offenders*. It implies importance of understanding line between the two types and processes of cross-over. Anyhow, they fail to distinguish if the offender is involved into small-scale crime or is professional criminal taking part in organized crime.

5.2 Non-contact and contact offenders

Research of Kettleborough and Merdin (2017) implies that the most frequent implicit theories of CSEMOs as defined by Ward and Kennon (1999) are: child as sexual being, entitlement and uncontrollability, while themes of dangerous world and na-

ture of harm were less influential. CSEMOs also have two subthemes: that children on pornographic materials are not real, and that children are actors that portray sexually aroused behaviour. On the other hand, Paquette and Cortoni (2020) found that theory about nature of harm is characteristic of CSEMOs even more than of CSSOs. Theory of world as dangerous place and of nature of harm is though more frequent with contact child sex offenders (CSOs) (Merdian et al. 2014) and CSSOs (Paquette & Cortoni, 2020).

Babchishin et al. (2015) found in their meta-analysis of researches on characteristics of CSEMOs that CSOs display significantly stronger emotional identification with children than CSEMOs. They identified that sexual interest in children, access to children, high levels of antisocial behaviour, and less psychological barriers to acting out a sexually deviant interests are main predictors that CSEMO develop into CSOs.

Brown and Brickel (2018) conducted meta-analysis of studies in five databases describing CSEM users. They found that CSEMOs: are predominantly male, 35% to 69% are single, tend to be older than the average offender which is 36-45 years, their race is white, their level of education are higher than other offenders, most of them are employed and many in professional positions; they also have poor mental health - 54% of them experienced depression and 35% have anxieties and phobias. CSEMOs have belief system that justify specific behaviour. Compared with CSOs and mixed sex offenders, CSEMOs “..are less assertive, less dominant, less socially confident or connected and less able to manage their emotions” (Brown & Brickel, 2018:6).

5.3. Cross-overs

Wolak et al. (2005) found in national U.S. study that out of 241 legal cases involving possessors of abusive images of children, 40% had committed also a contact sex offence against a child, while further 15% had attempted to do it. Authors suggested “a correlation between simple possession and committed sexual abuse of a child” (Wolak et al., 2005:6). Alexy, Burgess, and Baker (2005) found that 19% of study participants were mixed type - both traders (CSEMOs) and trawlers (CSOs). Self-admissions of contact offences by offenders charged with non-contact CSA was detected in U.S. much more frequently - in around 80% of the cases (Hernandez 2000 and 2006, cited by Beech et al., 2008:223).

Several processes facilitate move from non-contact to contact offences. Waste majority of pornographic child images accessible on the Internet normalize child pornography. Children smiling on abusive images allow offender to conclude that they are enjoying their sexualized exposure that lied to permission to cross the line. Membership into paedophilic community, step taken by many consumers of

CSA images, normalize contact offending. Fantasies induced by paedophilic images and subsequent masturbation and orgasm may fuel sexual desire toward children. Therefore, child pornography could promote both sexual attraction to children and self-justification of contact offences (Beech et al., 2008).

5.4. Child sex trafficking offenders

One of the best resources of data on CST offenders was U.S. national survey that included 1,416 persons arrested for sex trafficking of a minor in the United States from 2010 to 2015 (Roe-Sepowitz et al., 2017). It found that in 67.3% cases ICT was used in sex trafficking. Backpage.com was used in 41.8% cases. In most of the cases (3/4) only minor victims were involved, and traffickers were African American. Average age of the traffickers was 28.5 years with the trend of dropping over time. One-quarter of traffickers had a previous criminal history, most frequently violent crime. It is interesting that one-quarter of traffickers were females with a trend of increase in female sex traffickers. They are in average younger than male traffickers. More than a half (55.5%) of them had a role of a “bottom”, person that is also sex trafficked but is the most trusted by the main sex trafficker. “Bottom” may recruit victims, train them and give them rules and punishment.

In more than a half of cases traffickers recruited runaways. Their recruitment tactics included friendship, romance, offering place to stay, promises of material goods and giving psychoactive substances, but also sexual (18%) and physical (19.8%) assault. Usual place for trafficking was hotel room. Tactics of control of victims included threats of harm and psychological abuse (36.7%) and threats with a firearm (11.1%), sexual violence (36.3%), physical assault with a weapon (26.7%) and drugging (20.7%). Most of the cases of identification of trafficker (32,1%) were reaction to report to law enforcement by the victim, their family and anonymous caller, while on-fifth of the cases were identified through police stings.

6. RISK FACTORS FOR VICTIMIZATION

Some children are more vulnerable than other. Livingstone and Smith (2014:3) identified several risk factors for technology assisted CSA, including personality factors (sensation-seeking, low self-esteem, psychological difficulties), social factors (lack of parental support, peer norms) and digital factors (online practices, digital skills, specific online sites). Study of Jonsson et al. (2019:4) suggested association of online CSA with: lower socio-demographic background, previous experiences of emotional, physical and sexual abuse, psychological health,

troubled relationships with parents and some internet behaviours like sexting⁷. Hamilton-Giachritsis et al. (2017:20) found that 55% of the 216 young people had sent a sexual image of themselves to someone else before they were 16 years old. Of these, two thirds stated that they had felt forced to send at least some of these images, and 54% had sent at least some of these sexual images to someone over the age of 18. In a Swedish study of 18-year-old students, 20.9% had engaged in some form of voluntary sexual exposure online by posting pictures of themselves partially undressed, flashing, masturbating, or having sex on webcam (Jonsson, 2015:186). Reyns et al. (2011) emphasize that sexting is important predictor of becoming a victim of digital controlling behaviour (including sexual abuse) by an intimate partner.

Cyber dating as a sexual relationship with a person met online increases the risk of unwanted sexual contact (Mitchell et al., 2007). Study of Portuguese adolescents showed that cyber dating perpetration and victimization was associated with individual and intimate relation factors, while peer factors were associated only with cyber dating perpetration (Caridade & Braga, 2020).

Being a female, visiting chat rooms, discussing sexual topics online and sharing a personal information with a person they met online were related to receiving aggressive online sexual solicitation (Mitchel et al., 2007:7). Zweig et al. (2013) found that female students were more often victims of cyber sexual abuse, but they were less often victims of non-sexual cyber abuse. Female gender is strong predictor of a CST. Roe-Sepowitz, et al. (2017) found that 98,9% of minor victims were females.

Adolescent age is risk factor for CSA initiated online. That is likely due to more frequently use of the Internet and initial consensual creation of sexual images bound up with the increased risk-taking, impulsivity, sensation-seeking and sexual interest common to this life stage (Livingstone, et al., 2010). Adolescent age is also strong risk factor for sex trafficking (Statista, 2020, Roe-Sepowitz, et al., 2017).

According to international study of CSA *EU Kids Online* (Livingstone & Had-don, 2009:16) the ranking and frequency of risks for CSA among teenagers is very similar in different European countries. Giving out personal information was the most common risk everywhere, seeing violent or hateful content online was the third in the frequency ranking affecting one-third of teenagers, while being bullied or harassed online was the fourth, affecting one fifth of them. Receiving unwanted sexual comments and offline meeting with online contact were the last in the risk ranking. Lower socioeconomic status also increases the risk. Gender is risk factor, with boys more likely to seek out a pornographic or violent content,

⁷ Sexting is voluntary sending or receiving nude images of oneself.

meet somebody offline and give out personal information, and girls more likely to be upset by violent and pornographic content and to chat online with strangers.

Additional risk factors for CST victimization are: run away from home (Roe-Sepowitz, et al. (2017) and homelessness, physical and sexual abuse by family members, low socio-economic status (Child Trafficking Statistics, 2019), migration and war (Long, 2004).

7. CONCLUSIONS

This study aimed to analyze recent research on the prevalence of child sexual abuse exploitation and trafficking and overview existing typologies of technology assisted child sexual abuse including exploitation and trafficking. Data indicates that it is wide spread and grave phenomena with far reaching implication for victims and communities. Still it is hard to determine how many children experience online sexual abuse and to grasp its different forms and characteristics since many available studies are conducted in different languages with different methodologies. There is no agreed definitions of the scope of Internet offending (Taylor & Quayle 2010), online offending, online sexual abuse, online sexual exploitation and technology-assisted sex trafficking. These terms are often overlapping in its everyday use. Age of the children covered in the samples of different studies significantly varies. Anyhow, finding clearly indicate urgency in preventing and fighting technology-assisted child sexual abuse (CSA) and specially child sex trafficking. It is not easy to overcome barriers to effective preventions and interventions such as anonymity of users of CSA and traffickers, pace of evolving of information communication technologies and apps, accessibility and low cost of CSA to users and high profit of traffickers, as well as ad generational gap between children and their parent in using ICT and apps. Nevertheless, scope and consequences of CSA demand for development of a new more efficient approaches to combat the evil.

REFERENCES

1. Alexy, E. M., Burgess, A. W., & Baker, T. (2005) Internet offenders: Traders, travelers, and combination trader-travelers. *Journal of Interpersonal Violence*, 20, 804–812.
2. Anderson, M., & Jingjing J. (2018) *Teens Social media Technology*, Available at <https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/>, accessed on 4th April 2022

3. Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015) Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behaviour*, 44(1), pp. 45–66. doi:10.1007/s10508014-0270-x
4. Beech, A. R., Fisher, D., & Thornton, D. (2003) Risk assessment of sex offenders. *Professional Ark of Hope for Children* (2019) Child Trafficking Statistics, Last Updated: Tuesday, 09 April 2019 17. Available at <https://arkofhopeforchildren.org/child-trafficking/child-trafficking-statistics>, accessed on 30th April 2022.
5. Beech, A., Elliot, I., Birgen, A., & Findlater D, (2008), Internet and child sexual offending, *Aggression and Violent Behavior*, 13, pp. 216–228.
6. Brown R., & Bricknell S. (2018) What is the profile of child exploitation material offenders?. *Trends & issues in crime and criminal justice* no. 564. Canberra: Australian Institute of Criminology.
7. Caridade S, & Braga T, (2020) Youth cyber dating abuse: A meta-analysis of risk and protective factors. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 14(3), Article 2.
8. Charteris J., Sue G., & Masters Y. , (2014) Snapchat ‘selfies’: The case of disappearing data. Conference: *Proceedings ascilite Dunedin 2014* (pp. 389-393).At: Dunedin
9. Committee on the rights of the child (2019) Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, 10 September 2019
10. Council of Europe (September 2003) Group of Specialists on the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation, 136 pages. Available at https://ec.europa.eu/anti-trafficking/group-specialists-impact-use-new-information-technologies-trafficking-human-beings-purpose-sexual_en, accessed on 22nd April 2022.
11. Council of Europe (25 October 2007) *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, 2007 entered into force on 1st December 2009. Available at <https://www.humanium.org/en/council-of-europe-convention-on-the-protection-of-children-against-sexual-exploitation-and-sexual-abuse/>, accessed on 20th April 2022
12. Durkin, K., & DeLong, R. (2018) Internet-Facilitated Child Sexual Exploitation Crimes, *Encyclopedia of Information Science and Technology* (pp.1366-1375) Publisher: IGI Global

13. ECPAT International (2017) *Summary paper on online child sexual exploitation*, Available at: <https://.ecpat.org>, accessed 21.04.2022
14. Europol (2014) *Internet Organised Crime Threat Assessment (iOCTA) 2014*. The Hague: Europol.
15. Europol (2015) *Virtual Global Taskforce Child sexual exploitation environment scan, 2015*. The Hague: Europol.
16. Europol (2016) *Internet Organised Crime Threat Assessment (iOCTA)*. The Hague: Europol.
17. Europol (2020) *Exploiting isolation: Offenders and victims of online child sexual abuse during the Covid-19 pandemic*. Hague: Europol.
18. Hanson, E. (2019) 'Losing track of morality': Understanding online forces and dynamics conducive to child sexual exploitation. In J Pearce (Ed) *Child Sexual Exploitation: Why Theory Matters*, 87-116. Policy Press.
19. Hamilton-Giachritsis C., Hanson E., Whittle H, & Beech A. R. (2018) "Everyone deserves to be happy and safe": the impact of online and offline child sexual abuse, A mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it (PDF). London: NSPCC. Available at: <https://learning.nspcc.org.uk/research-resources/2017/impact-online-offline-child-sexual-abuse>, Accessed 29.04.2022
20. Hargrove D., Avitable R., Hsu N., & Dean M. (2022) 11 lesser known apps that experts say could expose your child to sex trafficking, Available at: <https://www.nbcsandiego.com/news/investigations/11-lesser-known-apps-that-experts-say-could-expose-your-child-to-sex-trafficking/2382725/>, Accessed: 22.04.2022.
21. Hartman, C. R., Burgess, A. W., & Lanning, K. V. (1984) Typology of collectors. In A. W. Burgess & M. L. Clark (Eds.), *Child pornography and sex rings* (pp. 93–109). Toronto: Lexington Books.
22. Heirman W., & Walrave M, (2008) Assessing Concerns and Issues about the Mediation of Technology in Cyberbullying, *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 2(2), 1. <https://cyberpsychology.eu/article/view/4214>
23. Hrcic, J. (2009) *Prestupništvo mladih: rizici, tokovi i ishodi*. Beograd: Institut za kriminološka i sociološka istraživanja.
24. Hrcic, J., & Loncar, N. (2016) Vršnjačko sajber nasilje među učenicima osnovnih škola, *Godišnjak Fakulteta političkih nauka*, Godna X, Broj 16, Decembar, 137-155; FPN, Beograd

25. Hrnčić, J., & Lončar, N. (2017) Parents involvement in cyber bullying experience of middle school students. *Nauka, bezbednost, policija*, 22. 23-45.
26. Jones L., Mitchell K, & Finkelhor D., (2012) Trends in youth internet victimization: Findings from three youth internet safety surveys 2000 - 2010. *Journal of Adolescent Health*, 50(2), 179-186.
27. Jones L., Priebe V., & Svedin G. (2015) Online sexual behaviours among Swedish youth: Associations to background factors, behaviours and abuse. *European Child & Adolescent Psychiatry*, 24(10), 1245-1260.
28. Jonsen L, Priebe C., & Svedin G. (2014) Voluntary sexual exposure online among Swedish youth – social background, Internet behavior and psychosocial health. *Computers in Human Behavior*, 30, pp.181-190. Children's Commissioner.
29. Kettleborough, D. G., & Merdian, H. L. (2017) Gateway to offending behaviour: Permission-giving thoughts of online users of child sexual exploitation material. *Journal of Sexual Aggression*, 23(1), pp. 19–32. doi: 10.1080/13552600.2016.1231852
30. Krone, T. (2004) *A typology of online child pornography offending. Trends and issues in crime and criminal justice*, 279, pp. 1–6.
31. Kooops, T.; Dekker, A.; Briken, P. (2018) Online sexual activity involving webcams-An overview of existing literature and implications for sexual boundary violations of children and adolescents. *Behavioral Sciences & the Law*, 36 (2), pp.182-197. DOI: 10.1002/bsl.2333.
32. Kuzmanović, D., Lajović, B. (2016). *Digitalno nasilje — prevencija i reaganje*, Beograd: Ministarstvo prosvete, nauke i tehnološkog razvoja, Kancelarija UNICEF-a u Srbiji, Pedagoško društvo Srbije.
33. Livingstone, Sonia and Haddon, Leslie (2009) *EU Kids Online: final report 2009*. EU Kids Online Network, London, UK. Available at: <http://eprints.lse.ac.uk/24372/> Accessed: 22th April 2022.
34. Livingstone S., Haddon L., Görzig A., Ólafsson K., (2011) *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. EU Kids Online, Deliverable D4. EU Kids Online Network, London, UK. Available at: <http://eprints.lse.ac.uk/33731> Accessed 21th February 2022.
35. Livingstone S., & Smith P., (2014) Annual research review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age, *Journal of Child Psychology and Psychiatry*, 55(6), pp 635–654

36. Long, L. D. (2004) Anthropological Perspectives on the Trafficking of Women for Sexual Exploitation. *International Migration*, 42(1), pp. 5 - 31
37. Mitchell K., Finkelhor D., & Wolak J. (2001) Risk Factors for and Impact of Online Sexual solicitation of Youth. *JAMA*, Vol 285, No.23:3011-3014. (American Medical Association).
38. Mitchell KJ, Finkelhor D, Jones LM, & Wolak J. (2012), Prevalence and characteristics of youth sexting: a national study. *Pediatrics*. 2012 Jan;129(1):13-20.
39. Mitchell, K.J., Jones, L.M., Finkelhor, D. & Wolak, J. (2014) *Trends in Unwanted Online Experiences and Sexting: Final Report*. 2014. Durham, NH: Crimes against Children Research Center.
40. Madden M., Lenhart A., Cortesi S., Gasser U., Duggan M., Smith A., & Beaton M. (2014) Teens social media and privacy Pew Research Center, Available at: <https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/> Accessed: 11th April 2022
41. Merdian, H. L., Curtis, C., Thakker, J., Wilson, N., & Boer, D. P. (2014) The endorsement of cognitive distortions: Comparing child pornography offenders and contact sex offenders. *Psychology, Crime and Law*, 20(10), pp. 971–993. doi:10.1080/1068316X.2014.902454
42. Medierådet, S.[The Swedish media council]. (2017) Unga och medier 2017 [Youth and media 2017]. <https://statensmedierad.se/publikationer/ungarochmedier/ungarmedier2017.2344.html>.
43. Mitchell KJ, Ybarra M, & Finkelhor D. (2007) The Relative Importance of Online Victimization in Understanding Depression, Delinquency, and Substance Use. *Child Maltreatment*.;12(4):314-324. doi:10.1177/1077559507305996
44. Paquette, S., & Cortoni, F. (2022) Offense-Supportive Cognitions Expressed by Men Who Use Internet to Sexually Exploit Children: A Thematic Analysis. *International Journal of Offender Therapy and Comparative Criminology*, 66(6-7), pp.647-669.
45. Parti K., Schmidt A., & Virag G. (2012) L' esperienza ungherese. In M. B. Morano & D. Valentino (Eds.), *Piu scuola meno mafia e cyberbullismo. Contrasto alle nuove forme di devianza giovanile* (pp. 77-83). *Annali della Pubblica Istruzione*, 6/2012. Firenze: Le Monnier
46. Prensky M. (2007). How to Teach with Technology: Keeping Both Teachers and Students Comfortable in an Era of Exponential Change. *Emerging Technologies for Learning*, 2, 40-46.

47. Reyns B., Henson B., & Fisher B. (2011) Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(11), 1149–1169.
48. Roe-Sepowitz, D., Gallagher, J., Hogan, K., Ward, T., Denecour, N., & Bracy, K. (2017) *A Six-Year Analysis of Sex Traffickers of Minors: Exploring Characteristics and Sex Trafficking Patterns*. Tempe, Arizona: Arizona State University.
49. Schulz van Endert, T, & Mohr, P.N.C. (2020) Likes and impulsivity: Investigating the relationship between actual smartphone use and delay discounting. *PLoS One*. 2020 Nov 18;15(11):e0241383.
50. Suler J. (1999) To get what you need: healthy and pathological internet use. *Cyber Psychology & Behavior*, 2, pp. 385–394.
51. Statista (2020) *Number of sex trafficking survivors in the United States in 2019, by age at time trafficking began*. Available at <https://www.statista.com/statistics/967429/sex-trafficking-survivors-age-time-trafficking-us/>, accessed on 19th April 2022.
52. Tan, O. S. L.; Khan, S., & Rahim, R.A. (2014) Internet: the double-edged sword of trafficking of women in Malaysia. *Pertanika Journal of Social Science and Humanities*, 22(S), pp. 149-160. DOI:10.1111/j.0020-7985.2004.00272.x
53. Quayle E., (2017) *Over the Internet Under the Radar*, Online child sexual abuse and exploitation a brief literature review, Available at: <https://www.cycj.org.uk/resource/over-the-internet-under-the-radar-online-child-sexual-abuse-and-exploitation-a-brief-literature-review/> accessed on 11th April 4.2022
54. Quayle E., & Taylor M., (2002) Child pornography and the internet: perpetuating a cycle of abuse, *Deviant Behavior*, 23:4, 331-361, DOI: 10.1080/01639620290086413
55. Wolak J., & Finkelhor D. (2011). *Sexting: A typology*. Durham, NH: Crimes against Children Research Centre.
56. United Nations International Children’s Emergency Fund (1989) *The Convention of the Rights of the Child*. New York: UNICEF.
57. U.S. Department of State (2000) *Victims of trafficking and violence protection act of 2000*. PUBLIC LAW 106–386—OCT. 28, 2000. Available at <https://www.govinfo.gov/content/pkg/PLAW-106publ386/pdf/PLAW-106publ386.pdf>, accessed on 20th April 2022
58. U.S. Department of State. (2015) *U.S. Laws on trafficking in persons*. Available at <http://www.state.gov/j/tip/laws/>, accessed on 21th April 2022.

59. Ward, T., & Keenan, T. (1999) Child molesters' implicit theories. *Journal of Interpersonal Violence*, 14(8), pp. 821–838. doi:10.1177/088626099014008003
60. Walsh W., Wolak J. & Finkelhor D. (2012) *Methodology report – 3rd National Juvenile Online Victimization Study (NJOV3): Prosecution study*. Durham, NH: Crimes against Children Research Center.
61. Web-Iq (2018) *Web-IQ newsletter*. Amsterdam: Web-IQ.
62. Wigginton C, Curran M. & Brodeur, C. (2017) Global mobile consumer trends: second edition Deloitte Touche Tohmatsu Limited;. *Deloitte: Global Mobile Consumer Trends*, <https://www2.deloitte.com/global/en/pages/technologymediaandtelecommunications/articles/gx-global-mobile-consumer-trends.html>.
63. Wolak J., Liberatore M., Levine., & Neil, F. (2014) Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse Negl.* eb;38(2), pp. 347-56. Nov 17. PMID: 24252746.
64. Zweig, J.M., Dank, M., & Yahner, J. (2013) The Rate of Cyber Dating Abuse Among Teens and How It Relates to Other Forms of Teen Dating Violence. *J Youth Adolescence* 42, pp. 1063–1077.

Prof. dr Jasna Hrnčić

Redovni profesor, Fakultet političkih nauka, Univerzitet u Beogradu

Nina Lončar, MA

JU Dom starih "Pljevlja", Crna Gora

SEKSUALNA ZLOUPOTREBA, ESKPLOATACIJA I TRGOVINA DECOM POSREDSTVOM INFORMACIONIH TEHNOLOGIJA

Seksualno zlostavljanje dece je jedan od najpogubnijih oblika ljudske komunikacije. Poslednjih decenija je ono olakšano informaciono-komunikacionim tehnologijama (IKT). Autori analiziraju karakteristike i specifičnosti seksualnog zlostavljanja dece uz pomoć IKT, uključujući eksploataciju i trgovinu decom, kako bi se bolje razumeo ovaj fenomen. Ispitani su osnovni pojmovi u oblasti seksualnog zlostavljanja dece koje se ostvaruje posredstvom IKT, analizirane su specifičnosti onlajn okruženja kao faktora rizika, prikazana je prevalencija fenomena. Objašnjene su implicitne teorije, kognitivne distorzije i motivacija prestupnika. Ispitane su aktuelne tipologije seksualnog zlostavljanja dece posredstvom IKT i počinitelaca, kao i faktori rizika za viktimizaciju. Razmatrane su razlike i preklapanja između termina i tipologija u ovoj oblasti i analizirane su prepreke za efikasnu prevenciju i intervencije. Istaknuta je važnost efektivne socijalne reakcije na ovo očigledno zlo.

KLJUČNE REČI: internet / seksualno zlostavljanje dece / seksualna eksploatacija dece / seksualna trgovina decom / tipologija / faktori rizika

PROTECTION OF CHILDREN VICTIMS OF SEXUAL VIOLENCE AND SEXUAL HARASSMENT IN BOSNIA AND HERZEGOVINA

Miodrag N. SIMOVIĆ, PhD¹
Azra ADŽAJLIĆ-DEDOVIĆ, PhD²

Sexual violence is always a serious violation of the victim's personality, autonomy, psychophysical integrity, self-control and self-esteem. Numerous other persons, thereby, including family members of victims, relatives, friends, acquaintances, etc., often appear as secondary victims. The prevalent victims of sexual violence in Bosnia and Herzegovina are female minors. Unlike sexual violence, sexual harassment is a delict of power aimed at "helpless victims" in non-democratic societies where there is no equality of rights for all citizens, but one part of society (men) seeks to maintain their positions of power by preserving the "patriarchal family" and sexual/gender discrimination and violence. The aim of this paper is to present the penal policy in the context of sexual violence against children in Bosnia and Herzegovina. In this regard, the protection of victims of sexual harassment and the results of the survey on fear of victimization - sexual violence and sexual harassment are analyzed. The results of the research should justify both the scientific and social significance of this paper.

KEY WORDS: children / violence / violence / penal policy

-
- ¹ Vice-president of the Constitutional Court of Bosnia and Herzegovina, Full member of the Academy of Sciences and Arts of Bosnia and Heregovina, Full professor, Faculty of Law, University of Bihać, miodrag.simovic@ustavnisud.ba
- ² Full professor, Faculty of Criminalistics, Criminology and Security Studies, University of Sarajevo, aadzajlic@fkn.unsa.ba.

1. INTRODUCTORY REMARKS

When it comes to the sexual, gender-based and sex-based violence, one can think of the victims of conventional crime or three special groups of victims. These are victims of sexual violence, then victims of sexual offenses and victims of sex-based violence.

Force or threat in most crimes of sexual violence is an act of committing these crimes. Force is the use of force against a person, aimed at forcing a person to take or not to take a certain action (doing or not doing). Absolute force (*vis absoluta*) is a force of such intensity that excludes any resistance and it is about the use of physical force against a person, and can be the use of hypnosis, alcohol, drugs, various aphrodisiacs and other intoxicants and ways to bring someone against his or her will into an unconscious state or a state that excludes any resistance. On the other hand, psychic force (*vis compulsiva*) exists when the use of force is carried out by threatening or pretending to be evil or intimidating. The victim's resistance is any action or reaction of the victim, which prevents or delays the attack of the sexual abuser, and can be passive, verbal and physical.

Proving sexual violence is particularly difficult and demanding since it requires speed and intensive cooperation between the police and prosecutors' when prosecuting sexual abusers with mandatory protection of the victim's identity. Therefore, these investigations must be accompanied by a label of urgency and secrecy in the proceedings, with mandatory supervision of the Prosecutor's Office over the undertaken activities of authorized officials, especially when it comes to the human trafficking and international recruitment for prostitution. Urgent detection of the prosecutor is necessary mostly because of some biological traces that are crucial for proving, could be permanently lost over time, but also because the prevalent victims of sexual violence in Bosnia and Herzegovina are children. Therefore, immediately upon the information that a child is a victim of sexual violence, the police are obliged to inform the service or social work center that is actively involved in the care and protection of the child together with non-governmental organizations (Archbold, et al, 2021: 18 -34).

2. MILD PENAL POLICY ENCOURAGES SEXUAL VIOLENCE AGAINST CHILDREN IN BOSNIA AND HERZEGOVINA

Bosnia and Herzegovina has been a member of the Council of Europe since 24 April 2002 and a signatory to the European Convention for the Protection of Human Rights and Fundamental Freedoms from 12 July 2002, since when has been

obliged to ensure proclaimed human rights and fundamental freedoms set forth in this Convention to all the persons under its jurisdiction. Article 2 paragraph 2 of the Constitution of Bosnia and Herzegovina stipulates that the rights and freedoms provided for in the Convention and its protocols are directly applicable and that these acts have priority over all other laws. The protection of human rights, referred to in Article 2 of the Constitution of Bosnia and Herzegovina is specifically regulated by other Annexes to the General Framework Agreement for Peace in Bosnia and Herzegovina, signed in Dayton in 1995, and these are Annexes 6 and 7, as well as Annex 1 to the Constitution of Bosnia and Herzegovina, which contains a list of 15 international documents and conventions in the field of human rights that will be applied in Bosnia and Herzegovina or that are legally binding for the state.

From the moment of signing the Convention, all control mechanisms of this Convention are applied. Article 8 of this Convention specifically stipulates that the state may interfere in the sphere of private life and thereby, in accordance with legally prescribed limitations, violate the right to privacy of every citizen of Bosnia and Herzegovina in order to protect the mental or physical integrity and life of every family member who is a victim of violence. In this regard, the Law on Gender Equality³ and the Law on Prohibition of Discrimination⁴ at the state level were adopted in Bosnia and Herzegovina, and new Entity family laws are in force as well, guaranteeing special protection of children as victims of discrimination and violations of children's rights.

Pursuant to the Criminal Code of the Federation of Bosnia and Herzegovina⁵, which has been in force since 1 August 2003, with certain amendments, criminal offenses related to sexual violence are covered by Chapter XIX of this Law entitled "Criminal Offenses against Sexual Freedom and Morality". The nineteenth chapter of the Criminal Code of the Federation of BiH includes Articles 203-213, and according to the articles, the following criminal offenses: rape, sexual intercourse with a helpless person, sexual intercourse by abuse of position, forced sexual intercourse, sexual intercourse with a child, lechery, satisfying lust in presence of a child or juvenile, pandering, abuse of a child or juvenile for pornography, introducing pornography to a child, and incest. Pursuant to the Law on Amendments to the Criminal Code of the Federation of BiH from 2016, Article 203 (rape) paragraph 4 was amended, according to which the penalty shall be applied for whosoever compels another person to have sexual intercourse with him by force or threat, out of hatred for the victim. Men-

³ "Official Gazette of BiH" Nos. 16/03, 102/09 and 32/10.

⁴ "Official Gazette of BiH" Nos. 59/09 and 66/16.

⁵ "Official Gazette of the Federation of BiH", Numbers 36/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 and 75/17.

tioned changes also included the change of duration of imprisonment, for gain or other benefits, induces, incites or lures another in offering sexual services or in another way enables their sexual intercourse over to a third person for the same reasons or in any way takes part in organizing or managing of sexual services offering for which a sentence of imprisonment for one to five years was prescribed.

When it comes to the rape, a person shall be sentenced to imprisonment for a term of one to ten years, and if this crime was committed in a particularly cruel or degrading manner, and if the raped person suffered grievous bodily injury or the raped person is a juvenile - stricter sanction or sentence of imprisonment from a term of three to 15 years. For the criminal offense of sexual intercourse with a helpless person, prescribed sentence is imprisonment for a term of one to eight years, for sexual intercourse by abuse of position from three months to three years, and for forced sexual intercourse from six months to five years.

Introducing pornography to a child, on the other hand, is punishable by a fine or imprisonment for a term of one year, while sexual intercourse or equivalent sexual act with a relative by blood in direct line or a sibling, shall be punished by a fine or imprisonment for a term between six months and two years. There is one exception in the case when the victim is a juvenile, and then a sentence of imprisonment for a term between one and five years is prescribed, or when a victim is a child - two to ten years of imprisonment.

There is still a legal provision in force by which sexual intercourse with a child, i.e. the exploitation of a child for committing sexual intercourse or other sexual acts is punished with imprisonment for a term of one to eight years. Sexual intercourse by abuse of position, i.e. inducing into sexual intercourse a person who is in subordinate or dependent position in relation to the perpetrator, shall be punished by sentence of imprisonment for a term of up to three years. Performing intercourse in a public place, that is, satisfying sexual passions in front of others - is punishable by a fine or imprisonment for a term of up to one year. If it is committed in front of a child or a juvenile, the punishment is a fine or imprisonment for a term of up to three years.

Furthermore, the abuse of children and juveniles for the production of audio-visual material (Gordon, 2021) or other pornographic contents shall be sentenced to imprisonment for a term between six months and five years, and, in doing so, confiscating all objects created or used, as well as intended for these purposes. On the other hand, the production and projection of such content, child pornography, materials showing pornographic performances in which children participate, shall be punishable by a fine or sentence of imprisonment for a term of up to one year. In the case of a person under the age of 16, the perpetra-

tor shall be sentenced to imprisonment for a term of up to three years (Gordon, Cochrane, 2020).

The Criminal Code of the Republika Srpska⁶ gives a definition of child pornography, meaning that pornographic material is a material that visually depicts a child or juvenile participating in evident sexual behavior or realistic photographs showing a child or juvenile participating in sexual behavior. Ultimately, if a person has sexual intercourse with a relative by blood, brother or sister, he or she shall be sentence by imprisonment for up to three years or a fine. If it involves a minor or a juvenile, the the prescribed penalty is sentence of imprisonment for a term between one and eight years, and as such it is treated almost equally as sexual violence against a child. Criminal sanctions will not be applied against the victim of this crime if she was under aged at the time of the commission, which is also valid in the case when the crime continued after the victim became an adult.

3. PROTECTION OF VICTIMS OF SEXUAL HARASSMENT

Sexual harassment is a form of sex discrimination that violates, among the other legal acts, Chapter VII of the 1964 US Civil Rights Act⁷ and this forms is a widespread social problem. A 1994 US Board of Merit Protection survey found that more than 40 percent of female workers and 19 percent of male workers reported experience of unwanted sexual attention, but only six percent of those who experienced sexual harassment took formal actions. The Equal Employment Opportunities Commission (EEOC) received almost 13,000 complaints of sexual harassment in 2007, and 16 percent of those complaints were filed by male workers. In the educational setting, a 2001 and 2005 survey by the American Association of University Women found that 81 percent of high school students and 62 percent of students reported being sexually harassed. Although a higher proportion of younger girls experienced this form of victimization, male and female students were mistreated equally, but in different ways.

Traditionally, sexual harassment was considered a personal and private problem. The term “sexual harassment” was coined in 1975 by a group of feminists led by lawyer Catherine McKinnon, but early court disputes had difficulties in finding

⁶ “Official Gazette of the Republika Srpska”, Numbers 64/17, 104/18, 15/21 and 89/21.

⁷ Also known as Pub.L. 88–352, 78 Stat. 241, which entered into force on 2 July 1964. It is a federal law that put out of force greater forms of discrimination against racial, ethnic, national and religious minorities, as well as women. The law ended inequalities in voter registration requirements and racial segregation in schools, work and in public institutions

support for the allegation of sexual harassment as a form of sexual discrimination under Title VII of the 1964 Civil Rights Act. In 1980, the EEOC formulated guidelines defining sexual harassment to resolve the confusion that results from different understandings of sexual harassment.

Sexual harassment can have many forms and is not limited to requests for sexual services under threat of harmful consequences for the job if the employee refuses to comply with the requests. Victims of harassment do not have to show that they were not employed, that they were denied promotion, or were fired for refusing to engage in sexual activity. This form of harassment, in which the victim suffers a concrete economic loss due to non-fulfillment of sexual requirements, is simply one of the manifestations of sexual harassment, although it is especially obvious and ugly⁸.

Over the time, the definition of sexual harassment has continued to develop to reflect a better understanding of the ways sexual power acts in society. For example, it is well established that harassment and discrimination based on sex do not always have to be of sexual nature. Behavior that is not explicitly sexual may still be sexual harassment. The situation must be observed in the overall context.

According to the data of the Prosecutor's Offices in BiH, from 2018 to 2020, there were 50 reported cases of sexual harassment. The result is 18 indictments and 12 suspensions of the investigation⁹.

The following list is not final, but would help in identifying what is sexual harassment and sex-based harassment:

- demanding hugs;
- invasion of personal space;
- unnecessary physical contact, including unwanted touching, etc.;
- derogatory language and/or comments towards women (or men, depending on the circumstances), derogatory names related to sex;
- grumpiness or inappropriate staring¹⁰;

⁸ It has been established that subjecting a woman to negative treatment due to the perception, that she is not physically attractive and that it is not in accordance with the stereotype ideal of female beauty - is sexual harassment.

⁹ <https://hcabl.org/ne-postoji-opravadanje-za-seksualno-uznemiravanje/>, accessed on 15 March 2022.

¹⁰ According to the data of the Polyclinic for the Protection of Children and Youth of the City of Zagreb and Brave Phone, conducted in 2004, 2008 and 2013 (Brave Phone, 2014), 90 percent of children use the Internet and 93 percent of children use Facebook profile, with every second child having no supervision during its use. These studies show that almost every third child was exposed to messages with sexual content, with a third of them not confiding their experience to anyone.

- gender-related comment on a person's physical characteristics or manners¹¹;
- comments or behavior related to someone's perceived inconsistency with the gender role stereotype;
- showing or circulating pornography, sexual images or cartoons, sexually explicit graffiti¹² or other sexual images (including online)¹³;
- sexual jokes, including the dissemination of written sexual jokes (e.g. by e-mail)¹⁴;

- ¹¹ The objectives of the Council of Europe are to raise public awareness of the problem of sexual abuse and exploitation of children, and promote the Lanzarote Convention, in order to protect children as victims of crime as effectively as possible and prevent any form of stigmatization. Data from the Council of Europe show that one in five children is a victim of some form of sexual violence. <https://mup.gov.hr/vijesti/europski-dan-zastite-djece-od-seksualnog-zlostavljanja-i-iskoristavanje/287374>, accessed on 21. March 2022.
- ¹² According to the Manager of the program for the protection of children "Save the Children", A.B., statistics in the Great Britain show that only five per cent of cases of sexual abuse have been reported, meaning that the number of known cases of sexual violence against children is just "the tip of an iceberg". Pointing out that sexual violence against children can also be committed by children, she stated that it is wrong to think that only man can commit sexual violence against children. "Namely, at least 20 percent of women do that", B. told for Oslobodjenje. <https://www.tacno.net/diskriminacija/u-bih-nema-baze-podataka-o-seksualnom-zlostavljanju-djece/>, accessed on 19 March 2022.
- ¹³ A report released by Europol in June 2017 stated that this type of violence has been on the rise in recent years, and that the victims are even children of the age of seven. Extortionists are more likely to ask explicit videos and photographs from young girls, and money from young boys, which is a relatively new trend in the sexual abuse of children on the Internet. Another novelty is that the perpetrators require the child to include other children - brothers and sisters or friends - when photographing or filming. Thus, children who otherwise use the Internet in a safe way, as well as small children who do not yet use the Internet themselves, are in danger, and could actually not be accessed this way. <https://www.medijiskapismenost.hr/kratki-film-otkriva-kako-dje-ca-postaju-zrtve-seksualne-ucjene-na-internetu/>, accessed on 15 March 2022.
- ¹⁴ The establishment of the first Center for Safe Internet in Bosnia and Herzegovina in 2018 is the most significant result of a three-year project designed against sexual violence against children online, according to the implementers of this project entitled "Stop Violence against Children: Preventing and Combating Sexual Exploitation and Child Abuse in Digital Environment in BiH (EVAC)". Project Coordinator from the International Solidarity Forum (EMMAUS) B.G. at the press conference in Sarajevo, also stated that protocols had been signed with the Federal Police Administration, the Ministry of Internal Affairs of the Republika Srpska, and the Brčko District Police in order to prevent and suppress this type of violence. The result is a very good cooperation between the NGO sector and public institutions in this case, said the organizers of the press conference, and reminded that EMMAUS, together with UNICEF and Save the Children organization, began realization of the project in question three years ago. <https://dnevni.ba/vijesti-bih/bih/projekt-o-zastiti-djece-od-seksualnog-nasilja-u-digitalnom-okruzenju/>, accessed on 25 March 2022.

- rude and vulgar humor or gender-related language¹⁵;
- sexual or gender-related comment or behavior used to harass a person¹⁶;
- suggestive or offensive remarks or insinuations about members of a certain sex¹⁷;
- spreading sexual rumors (including online)¹⁸;
- propositions of physical intimacy;
- verbal abuse, threats or mockery related to sex¹⁹;

¹⁵ The first online lecture was held on 12 November 2020, via the Zoom application, on the topic “Violence against children in the digital environment”. Ass. A.D. gave the first part of the lecture on the given, who spoke about the Internet as an important part of social life of children and youth, and in which modern way technology is used. She went on talking about cyber dangers, forms of cyber-bullying, specific characteristics of how cyberbullying is happening, who are the most common victims, etc. The lecture and interactive workshop had a special focus on forms of cyberbullying, with a focus on hate speech, threatening messages and attacks on children from vulnerable categories of society. After discussion and lectures, the next lecturer was ass. M.S. from International Burch University. In: “Media literacy of parents about dangers of cyberspace for children and youth” 1 July 2020 – 31 December 2020, Sarajevo, The project was supported by the Federal Ministry of Education and Science.

¹⁶ In 2013, as a second-grade high school student, she was exposed to the unpleasant compliments of a professor who told her that she had a body like a goddess, and that on one occasion, when she entered his office to wash a ball. He used the opportunity and grabbed her buttocks, which caused anxiety, discomfort and a sense of threat to her sexual integrity, and because of such a feeling, she decided to report it to her parents and class teacher. Twelfth Case - Judgment of the Basic Court in Bijeljina, No. 80 0 K 069119 15 K of 25 March 2016, In: Mujezinović, 2021.

¹⁷ The socio-political environment is such that sexual harassment, as a form of violence against women is most easily tolerated, and in most cases, it remains unreported and there is no mechanism for sanctioning it. It is often treated as a trivial problem that can be easily avoided and stopped, which is usually not true. More on: <https://bljesak.info/vijesti/crna-kronika/seksualno-uznemiravanje-u-bih-mizerne-kazne-osuda-drustva-i-upiranje-prstom/361996>, accessed on 29 March 2022.

¹⁸ *A. v. Quality Inn*, (1993), 20 C.H.R.R. D/230 (Ont. Bd. Inq.); *Farris v. Staubach Ontario Inc.*, 2011, *supra*, note 23.

¹⁹ In Bosnia and Herzegovina, however, the most famous case is of a hodja from Gluha Bukovica, near Travnik, who fornicated with girls. The case received a court epilogue - R.O. served 18 months in prison. The scale of this crime is that the whole village defended the hodja, and the Islamic Community stood by him. None of them understood the accusation of the girl, who gained strength to say: “He was telling me to hold him by the genitals. He told me that if I said that, my mother would die.” Children victims of sexual abuse - Radio Free Europe, <https://www.slobodnaevropa.org>, accessed 30 March 2022.

- bragging about sexual power²⁰;
- required dating or sexual services²¹;
- questions or discussions about sexual activities²²;
- requiring employees to dress in a sexualized or gender-specific way²³;
- paternalistic behavior based on sex that the person considers to undermine his or her status or position of responsibility²⁴;
- threats to punish or otherwise prosecute a person who refuses to obey sexual efforts (known as retaliation) ²⁵.

²⁰ This happened when the public learned about several cases of sexual abuse and harassment of protégés of the Banja Luka Home for Children and Youngsters without Parental Care “Rada Vranješević”, by employees of this institution.

All this resulted in the resignation of the Director and the removal of the Board of Directors of the Home, but the question remains whether institutions such as this adequately implement preventive measures to protect children from sexual abuse and harassment. <https://ba.voanews.com/a/brojne-banjalucanke-otkrile-da-su-seksualno-uznemiravane-kao-djevojke/-6476656.html>, accessed on 30 March 2022.

- ²¹ Cases of abuse at the Sarajevo Faculty of Law, i.e. its departments in Zenica and Tuzla, are discussed in the Facebook group #NisamTražila (#IDidNotAskForIt). Not just about that faculty. Hundreds of anonymous testimonies of current and former female students are shared anonymously on social networks. Taken from: <https://www.slobodnaevropa.org/a/lavina-anonimnih-svjedo%C4%8Danstava-za-seksualno-zlostavljanje-na-fakultetima-u-bih-%C4%8Dekaju-se-prijave>, 10 April 2022.
- ²² Repeated and negative comments of a male employee to a female colleague from work about her physical appearance and the fact that he thinks she is overweight - is sexual harassment.
- ²³ *Mottu v. MacLeod and others*, 2004 B.C.H.R.T. 67 and *Bil v. Northland Properties*, 2010 B.C.H.R.T. 234.
- ²⁴ Sexual harassment is based on gender-based hostility and is often an attempt to make the target undesirable in his or her environment.
- ²⁵ During an average day, women spend an incredible amount of time and energy trying to avoid sexual harassment, and thanks to recent research, we now know how much. This time and effort is called “security work”, and it is: all those moments of self-censorship, adjusting our behavior, choosing what we wear or where we go, not based on our real desires, but fear for our safety, and those are not just minor obstacles. They have a major impact on our mental health, from everyday stress to serious effects like post-traumatic stress disorder. <https://en.abeachreefmotel.com/how-much-effort-do-women-put-into-coping-with-sexual-harassment-day>, accessed on 7 April 2022.

For example, a young single mother who receives social assistance and has had difficulty finding suitable accommodation for herself and her child may be very vulnerable to sexual harassment. If she is a racial or disabled person, her experience of harassment may be even worse²⁶.

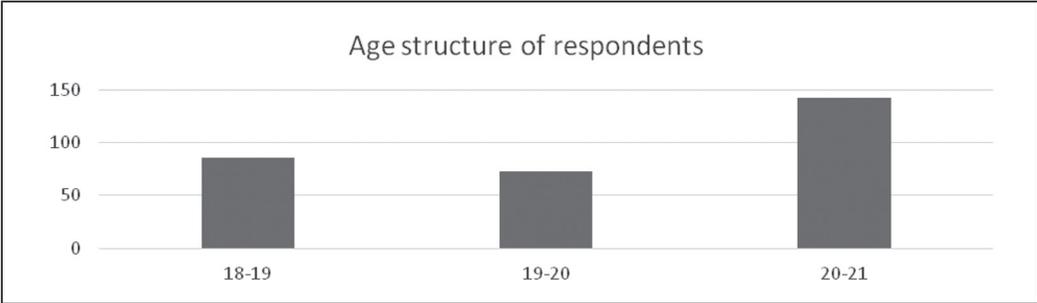
4. RESULTS OF THE SURVEY ON FEAR OF VICTIMIZATION - SEXUAL VIOLENCE AND SEXUAL HARASSMENT IN BOSNIA AND HERZEGOVINA

In order to determine the approximate extent of sexual violence in Bosnia and Herzegovina, we conducted a survey with students of the University of Banja Luka by surveying 301 students aged 18 to 21 who were randomly selected.

Table 1. Age structure of respondents

Characteristics of respondents	18-19	19-20	20-21
Total	86	73	142

Graph 1. Age structure in the survey

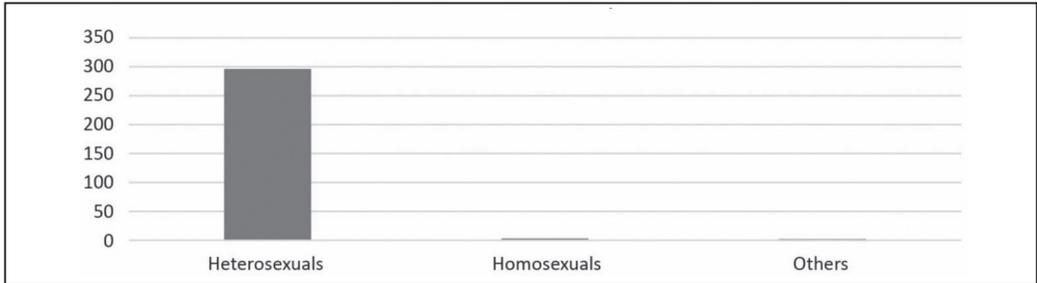


²⁶ The OHRC has explored this “contextualized” or “intersectional” approach to discrimination analysis at length in its Discussion Paper entitled *An Intersectional Approach to Discrimination: Addressing Multiple Grounds in Human Rights Claims*, available at: https://www.ohrc.on.ca/en/resources/discussion_consultation/DissIntersectionalityFtnts/view. (Retrieved: 17 April 2013). The concept of “intersectionality” has been defined as “intersectional oppression [that] arises out of the combination of various oppressions that, together, produce something unique and distinct from any one form of discrimination standing alone...” (Eaton, 1994: 203-229).

Table 2. Gender structure of respondents

Characteristics of the respondents	Heterosexuals	Homosexuals	Others
Total	296	3	2

Graph 2. Gender structure of respondents

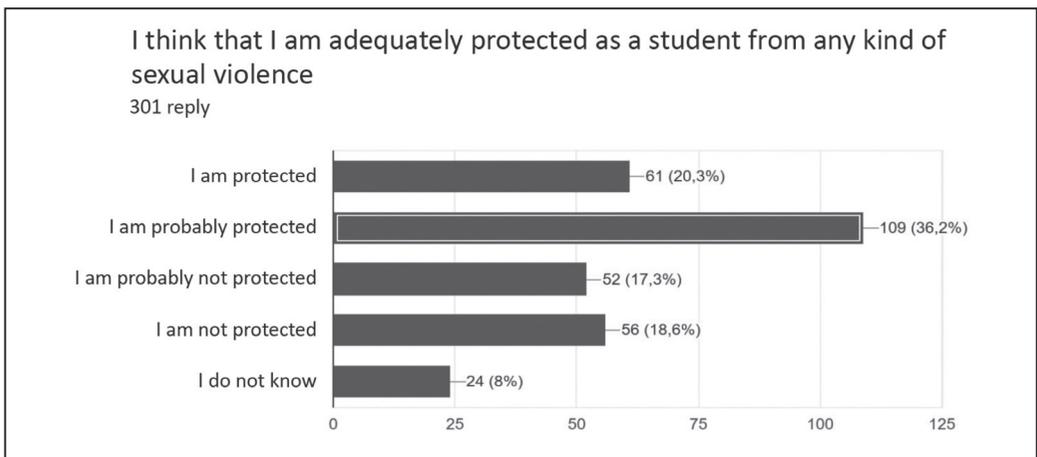


The majority or 99 percent of the respondents were heterosexuals, of which 165 were women and 136 were men. A common feature of all the respondents is that they were sexually harassed.

After presenting the structure of the respondents, we present the answers to specific questions in this survey conducted in 2021 in the period from 1 March until 1 June 2021 at the University of Banja Luka. The survey was conducted by the Banja Luka Research Center, which processed the results of the survey (survey questionnaires).

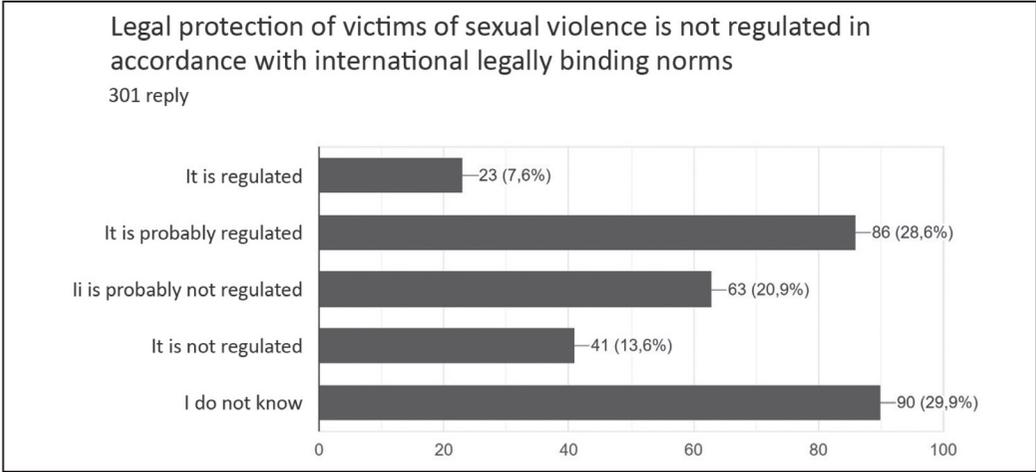
Through the Likart scale, we examined the positions and fears of the respondents through the following questions:

Graph 3. Legal protection against sexual harassment in Bosnia and Herzegovina



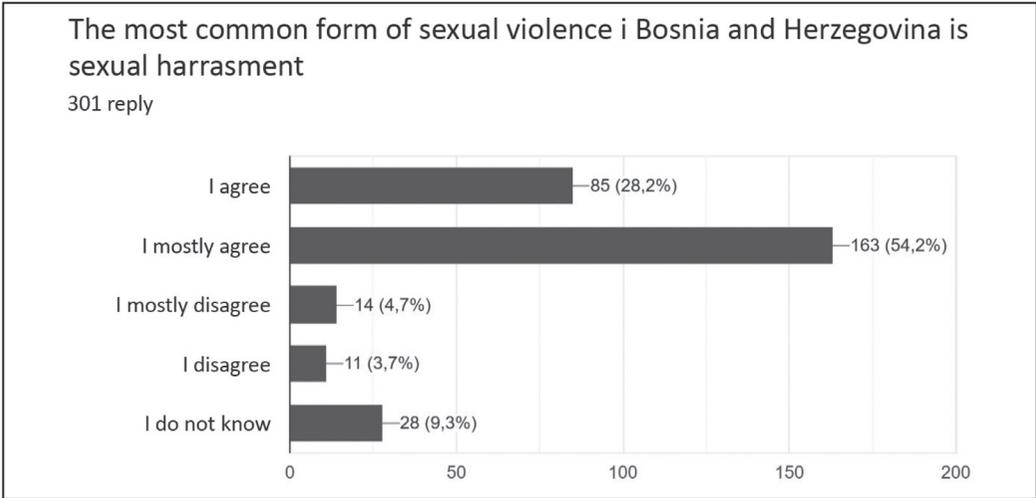
We conclude that the respondents feel protected and safe in Bosnia and Herzegovina because 170 of them answered that they felt very protected, which is 55 percent of the respondents.

Graph 4. Compliance of legislation with international legal norms in Bosnia and Herzegovina



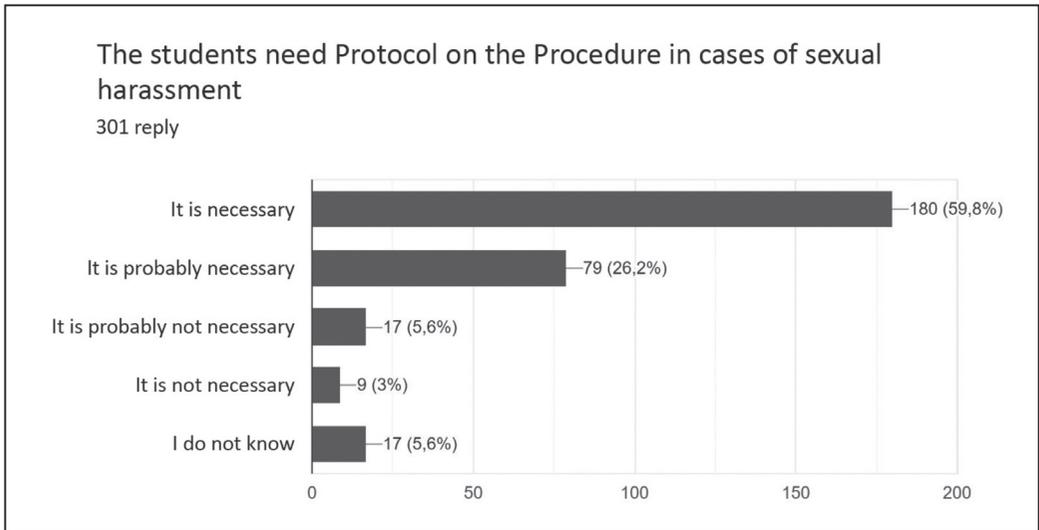
We conclude that the majority of the respondents, or 192 of them, believe that the legal protection of victims of sexual violence is not regulated in accordance with internationally legally binding norms, which is about 70 percent.

Graph 5. Prevalent form of sexual violence in Bosnia and Herzegovina



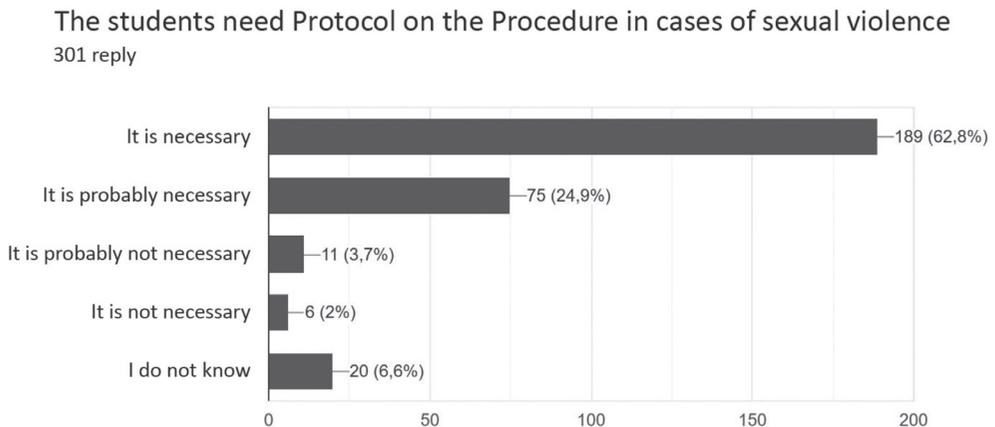
We conclude that the prevalent form of sexual violence or the most pronounced sexual violence in Bosnia and Herzegovina is “sexual harassment”.

Graph 6. Victimological measure of sexual harassment prevention in Bosnia and Herzegovina



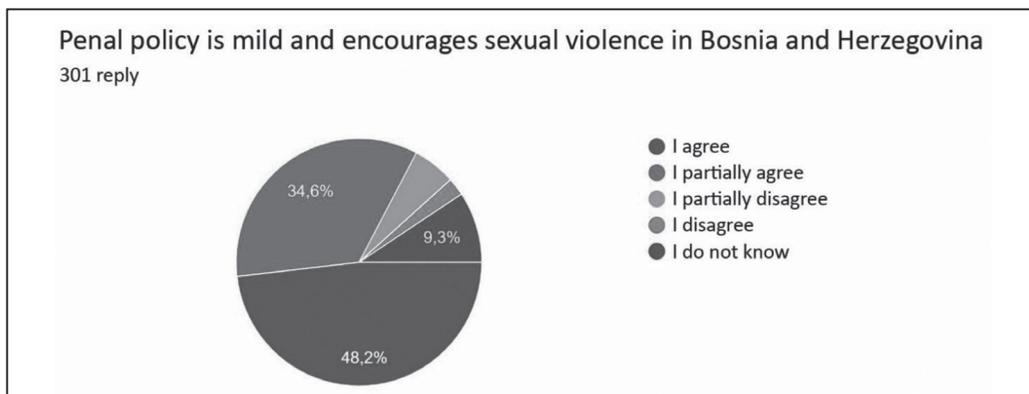
We conclude that the majority of the respondents, or 259 of them, proposed the development of a Protocol on the Procedure for the Protection of Victims of Sexual Harassment in Bosnia and Herzegovina.

Graph 7. Victimological measure of prevention of sexual violence in Bosnia and Herzegovina



We conclude that the majority of the respondents, 264 of them, proposed the development of a Protocol on the Procedure for the Protection of Victims of Sexual Violence in Bosnia and Herzegovina

Graph 8. Penal policy related to prevention and suppression of sexual violence in Bosnia and Herzegovina



We conclude that out of 301 surveyed students, 82.2 percent agree that the penal policy related to the prevention and suppression of sexual violence in Bosnia and Herzegovina is more than mild, and that punishments should be intensified, especially for violence against children victims of sexual violence and for attempted sexual offenses.

5. DISCUSSION

When we talk about sexual violence, from a victimological point of view, we are talking about victims of conventional crime, but sexual violence can be committed in war, as mass ethnic rape with characteristics of genocide and crimes against humanity or as war rape and then it is about the victims of severe violations of international humanitarian law, which is under the jurisdiction of the Court of BiH in BiH. Other sexual violence is defined by various laws in Bosnia and Herzegovina as sexual offenses, sexual violence and organized sexual exploitation that severely violate human rights and multiply victimize its citizens, such as trafficking and international recruitment for prostitution (or trafficking for prostitution).

Trafficking in human beings, especially juveniles, as well as international recruitment for prostitution, are serious crimes characterized by collective victims (multiple victims), multiple victimization of victims and long-term victimization. International documents mandate the definition of trafficking in such a way that the victim's consent to sexual exploitation is irrelevant to the "status" of victim, i.e. all victims found in these facilities are "forced victims of trafficking". In addition, international documents (PUP, 2012 and Istanbul Convention) ordered the establishment of centers for victims of sexual violence (for screening, gathering

evidence and providing medical assistance to victims) and departments for assistance, support and protection of these victims in the treatment of victims during criminal proceedings. It is also ordered that the states should provide efficient compensation systems for these victims by the state, which was not done in BiH because the law on compensation to victims of crimes was not adopted, and thus forming of a fund from which compensation would be paid to these victims, which certainly is a secondary victimization of victims, but also a violations of international obligations arising from Annex 1 to the Constitution of Bosnia and Herzegovina, and a number of international and European documents ratified by BiH. It is true that there is a Witness Support Unit in the Court of BiH, as well as laws and bylaws that are only partially in line with European legal norms and standards, but there is no adequate organizational and financial support, which can lead to multiple victimization of victims in each of these cases, for which individuals and the state of Bosnia and Herzegovina will be responsible.

Victims of gender-based and sex-based violence are “invisible victims”. More precisely, thanks to strong campaigns of female NGO and government representatives, domestic violence is recognized as a special form of gender-based violence, with sexual violence as a special form of domestic violence being neglected or statistically invisible due to stereotypes and prejudices that “there is no marital rape” or “a husband cannot rape a wife”, but we will stop here because our topic is not domestic violence and related sexual violence between marital and extramarital partners, but all other forms of gender-based and sex-based violence, the most pronounced of which is sexual harassment, discrimination based on gender and sex, mobbing and street harassment, which is also accompanied by a large “dark number” because the competent state and public officials do not recognize them, and citizens do not report them for various reasons. At the same time, there is a misconception (real and legal) among citizens and civil servants that all acts of discrimination, including discrimination based on gender and sex, are within the jurisdiction of the Office of the Ombudsman of Bosnia and Herzegovina, and that the police and Prosecutions should not do anything here, which is the most common cause of secondary victimization of victims.

REFERENCES

1. Archbold, L, Verdoodt, V., Gordon, F. & Clifford, D. (2021). Children’s Privacy in Lockdown: Intersections between Privacy, Participation and Protection Rights in a Pandemic, *Law, Technology and Humans*, 3(1), pp. 18-34
2. Eaton, M. (1994). Patently Confused, Complex Inequality and *Canada v. Mossop*”, *1 Rev. Cons. Stud.*

3. Gordon, F. (2021). The Rights of Children in the Digital Environment, Diplomacy Training Programme 2 June 2021, Australian National University, <https://www.oecd.org/sti/ieconomy/protecting-children-online.htm>.
4. Gordon, Cochrane, J. (2020). Submission in Response to the United Nations Committee on the Rights of the Child's Call for Comments on the General Comment on Children's Rights in Relation to the Digital Environment.
5. Mujezinović, J. (2021). Krivičnopravna zaštita, pravni i socijalni položaj žrtava seksualnog nasilja u Bosni i Hercegovini. *Osnovna studija Mujezinović, J., Marković, I., Begić, B., Fondacija "Lara", Bijeljina i Fondacija lokalne demokratije, Sarajevo.*

Internet sources

1. <https://hr.abeachreefmotel.com/how-much-effort-do-women-put-into-coping-with-sexual-harassment-day>
2. <https://hcabl.org/ne-postoji-opravljanje-za-seksualno-uznemiravanje/>
3. <https://www.slobodnaevropa.org>
4. <https://dnevni.ba/vijesti-bih/bih/projekt-o-zastiti-djece-od-seksualnog-nasilja-u-digitalnom-okruzenju/>
5. <https://www.medijskapismenost.hr/kratki-film-otkriva-kako-djeca-postaju-zrtve-seksualne-ucjene-na-internetu/>
6. <https://ba.voanews.com/a/brojne-banjalucanke-otkrile-da-su-seksualno-uznemiravane-kao-djevojke/6476656.html>
7. <https://www.slobodnaevropa.org/a/lavina-anonimnih-svjedo%C4%8Danstava-za-seksualno-zlostavljanje-na-fakultetima-u-bih-%C4%8Dekaju-se-prijave>
8. <https://www.vecernji.hr/sport/sportas-rodod-iz-bih-izbacen-iz-olimpijskog-sela-optuzili-ga-za-seksualno-uznemiravanje-1510320> - www.vecernji.hr
9. <https://bljesak.info/vijesti/crna-kronika/seksualno-uznemiravanje-u-bih-mizerne-kazne-osuda-drustva-i-upiranje-prstom/361996>
10. <https://www.tacno.net/diskriminacija/u-bih-nema-baze-podataka-o-seksualnom-zlostavljanju-djece/>,
11. <https://mup.gov.hr/vijesti/europski-dan-zastite-djece-od-seksualnog-zlostavljanja-i-iskoristavanja/28737>
12. https://www.ohrc.on.ca/en/resources/discussion_consultation/DissIntersectionalityFtnts/vie

Akademik prof. dr Miodrag N. Simović
Sudija Ustavnog suda Bosne i Hercegovine, redovni profesor Pravni fakultet,
Univerzitet u Bihaću, Bosna i Hercegovina

Prof. dr Azra Adžajlić - Dedović
Redovni profesor, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije,
Univerzitet u Sarajevu, Bosna i Hercegovina

ZAŠTITA DJECE ŽRTAVA SEKSUALNOG NASILJA I SEKSUALNO UZNEMIRAVANJE U BOSNI I HERCEGOVINI

Seksualno nasilje uvijek predstavlja tešku povredu ličnosti žrtve, njene autonomije, psihofizičkog integriteta, samokontrole i samopoštovanja. Nerijetko se, pri tome, kao sekundarne žrtve javljaju brojne druge osobe počev od članova porodica žrtava, rodbine, prijatelja, poznanika i dr. Prevalentne žrtve seksualnog nasilja u Bosni i Hercegovini su ženske maloljetne osobe. Za razliku od seksualnog nasilja, seksualno uznemiravanje delikt je moći usmjeren na "nemoćne žrtve" u nedemokratskim društvima u kojim nema jednakosti u pravima za sve građane, već jedan dio društva (muškarci) nastoje zadržati svoje pozicije moći kroz očuvanje "patrijarhalne porodice" i polnu/i rodnu diskriminaciju i nasilje. Cilj rada jeste i prikaz kaznene politike u kontekstu seksualnog nasilja nad djecom u Bosni i Hercegovini. S tim u vezi, analiziraju se zaštita žrtava seksualnog uznemiravanja i rezultati ankete o strahu od viktimizacije – seksualnog nasilja i seksualnog uznemiravanja. Rezultati istraživanja bi trebali opravdati kako naučni, tako i društveni značaj ovog rada.

KLJUČNE RIJEČI: djeca / nasilje / uznemiravanje / kaznena politika

OFFENDERS AND THEIR FAMILIES IN A DIGITAL ENVIRONMENT: A CASE STUDY OF PCI SREMSKA MITROVICA¹

Nikola VUJIČIĆ, MA²
Nikola DRNDAREVIĆ, MA³

The article provides a review of the developments and characteristics of video visitation in PCI Sremska Mitrovica, with a focus on the contact between offenders and their families and children. The study draws upon data from fieldwork interviews with the prison employees and aims to understand experiences of using video visitation and their importance in the offender behavior as well as the prison system. The study gives voice to field experts with the knowledge and skills to suggest how video visitation impacts the offender behavior and its relevancy in the context of familial relationships. Moreover, it reflects on the nature of digital technologies in prisons and considers how they are embraced and managed in Serbia. Special focus is on the legislative framework in the Republic of Serbia.

KEY WORDS: prisons / digital environment / video visitation / family contact / children

-
- ¹ This research was supported by the Science Fund of the Republic of Serbia, Grant No. 7750249, Project title: Assessment and possibilities for improving the quality of prison life of prisoners in the Republic of Serbia: Criminological-penological, psychological, sociological, legal and security aspects (PrisonLIFE).
- ² Research Associate, Institute of Criminological and Sociological Research in Belgrade, nikola.vujcic.law@gmail.com
- ³ Research Assistant, Institute of Criminological and Sociological Research in Belgrade, thanness@gmail.com

1. INTRODUCTION

Society today is inevitably shaped by digital technologies in which there is a rapid movement toward the digital environment. The accelerating shift from analog to digital, the digital revolution, is enabled by the continuing progress in the areas of technology, that is affecting and reshaping both the environment and the people.

The prominent impact of digital society is reflected on crime and criminal justice as well as in prisons, calling for a different perspective. Certain terms have begun replacing or supplementing the existing ones to accommodate such a shift. The most recent one amongst scholars is the area of digital criminology (Kubiček et al., 2020). However, there seems to be insufficiency at the level of engagement between the criminological institutions with digital criminology and its various aspects (e.g. digital justice, investigation and evidence, surveillance, education, video conferencing...). Implications of a changing landscape initiate new methodological and ethical challenges as well as the modifications to the structure of society and the approach toward the topic of digital environments in the criminological field (Kubiček et al., 2020; Powell et al., 2018). To these complex changes, the area of criminology would benefit from a multidisciplinary perspective encompassing, among others, a legal reflection, psychology and behavioral science, criminology, sociology, and digital sciences.

It should be borne in mind that the forced nature of the prison environment means that punishment affects many aspects of everyday life in prison. Looking beyond the prison walls, convicts' relationships with their families have fundamentally changed and severely limited (Coyle, 2008: 220). Precisely, this means that convicts should be enabled to maintain quality contact with their families, especially with children who may be particularly vulnerable due to separation from their parents. The use of video technologies is just one of the ways that should be used for these purposes.

The United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) represent the most important document in this matter. In addition to a number of standards, Rule no. 58 provides that prisoners shall be allowed, under necessary supervision, to communicate with their family and friends at regular intervals: (a) By corresponding in writing and using, where available, telecommunication, electronic, digital and other means; and (b) By receiving visits. This Rule is important from the aspect of our analysis for two reasons: first, it clearly specifies that contact can be made through technical means and second, it is not an alternative, but an additional option in relation to receiv-

ing visits (face-to-face). In other words, the use of modern technologies is an addition to the already existing physical visits.

The prison systems have been affected by the digitization of society along with a broad range of aspects, some of which relate to digital criminality, offender education programs as well as the communication with outsiders, namely with the justice systems and with offenders' families. The prisons have been introducing digital technologies, within the limitations imposed by the law and financial and structural conditions of the institutions, intending to reduce the digital divide, improving digital inclusion, for the betterment of the resocialization processes (Järveläinen & Rantanen, 2020).

The structural characteristics of the prisons can accommodate the digital transformations at various levels, ranging from comprehensive solutions and concepts to incidental solutions concerning technology enabling communication as well as a dedicated space for video conferencing (Powell et al., 2018). Video conferencing for offenders has been used for various purposes such as attending the court hearings, reducing the transportation costs, medical examinations, and increasing and strengthening the offender-family contact and generally the contact to the outside world (Crabbe, 2002; Järveläinen & Rantanen, 2020).

The use of IT has penetrated so deeply into all aspects of private life, that it was quite to be expected that the IT revolution would also enter the criminal justice systems (Bugarski, 2021: 80). Precisely, the use of "online technologies" has led to a re-examination of how they affect the "right to access to justice", the "right to a fair trial" and the "fair administration of justice" (Miljuš, 2021: 229). In the domestic criminal law literature, the issue of the use of video links and other technical means is mainly considered from the aspect of criminal procedure legislation, and much less in the context of the execution of criminal sanctions, primarily imprisonment.

If the Law on Execution of Criminal Sanctions (*hereinafter: Law*)⁴ is considered as the basic law that regulates the treatment of persons sentenced to imprisonment, no provision provides for the explicit use of a video link, as a way of maintaining contact with family and / or other persons. It is interesting to mention here that the COVID-19 pandemic has contributed to the fact that under certain conditions, certain phases in criminal proceedings can be carried out using a video link. If the above is taken into account, a logical interpretation leads to the conclusion that there should be no obstacles for convicted persons to make contact with their families in a similar way. This attitude can be further justified by the fact that far greater practical and other problems are present during the main trial (*trial in the narrow sense*) than when maintaining contact with the

⁴ Law on Execution of Criminal Sanctions, Official Gazette RS, No. 55/14 & 35/19.

family, where we are not talking about court proceedings, but about exercising the rights of the convict.

A special form of maintaining contact with the family, which is not face to face, and which appears in our criminal executive legislation, is through telephone conversations. The provision of Article 88, paragraph 1 of the Law stipulates that the convicted person shall be entitled to telephone conversations in compliance with the provisions of the regulation governing the house rules of the penitentiary institution, at his/her own expense. In the next paragraph, a reference provision is provided for in Article 87 paragraph 2 of the Law, which introduces the possibility of supervision in closed and closed institutions with special security or in a closed ward of a penitentiary institution. So, the basic rule is that phone conversations are not monitored. The Rulebook of the house rules of penitentiary institutions and district prisons (*hereinafter: The House Rules*)⁵ stipulates that a convict who is classified in a closed ward may make telephone calls at least four times a week, and a convict who is classified in a semi-open and open ward may make daily calls, in accordance with the possibilities of the institution. The penitentiary institution should provide the required number of telephone booths; the call schedule is based on a pre-announced schedule and lasts up to fifteen minutes; the convicted person conducts the interview in the language of his choice and at his own expense. Telephony may be restricted only by a court, in accordance with the law (Article 38 of the House Rules).

As we often encounter the question of whether the virtual world of communication can be a substitute for seeing face to face, it is important to keep in mind how visits to convicts are regulated according to the provisions of the Law. First of all, the visits are regulated in the part of the Law that deals with the issue of the rights of a convicted person. The provision of Article 90 paragraph 1 of the Law, stipulates that convicted person shall have the right to visits by a spouse, children, parents, adopted children, adoptive parents and other lineal or collateral relatives up to the fourth degree of consanguinity or relatives by marriage up to the fourth degree of consanguinity, as well as of the foster parents, foster children and guardians once every two months. In the next paragraph, it is prescribed that the prison ward may approve visits to the convicted person by other persons as well. When it comes to the duration of visits, the provision of Article 93 of the Law stipulates that the minimum duration of a visit shall be one hour, where the time, duration, manner of visit and appearance of the visiting room are regulated by the House Rules.

⁵ Rulebook of the house rules of penitentiary institutions and district prisons, Official Gazette RS, No. 110/14 & 79/16.

The House Rules, among other things, stipulate that the visit to the convicted person is performed on Saturdays and Sundays and on non-working public holidays from 9:00 to 17:00. The duration of the visit longer than one hour must be approved by the prison ward. Also, the prison ward may approve visits on other days, if there are justified reasons for that (Article 45 of the House Rules).

Let's go back to the provisions of the Law. In addition to the right of the convict to make visits, which belongs to every convicted person, within the extended rights and privileges of the convicted person, the provision of Article 129 paragraph 1 point 2 of the Law, stipulates that the prison ward may grant an extended number of visits to a convicted person who behaves particularly well and tries hard and achieves progress against the sentence program. In the next point, the Law prescribes right to an extended circle of persons who may visit the convicted person (distant relatives, friends and others).

Rulebook on treatment, treatment program, classification and subsequent classification of convicted persons (*hereinafter*: The Rulebook of Treatment)⁶ provides that the extended right to a number of visits to a convict may be granted once a month, with no restrictions on treatment groups, when it comes to the extended right to a circle of persons who may visit a convict (Article 29 & Article 30 of the Rulebook of Treatment).

In maintaining the connection to the outside world and the family members, video visitation has become an important mechanism in the digital era. Due to the COVID-19 pandemic, face-to-face contact has been prohibited in many prisons, which has advanced video visitation into the foreground (Dallaire, 2021; Stickel et al., 2021). Face-to-face visitation also makes high demands on the families of offenders. Most prominently, prisons tend to be significantly distant from home, therefore incurring traveling costs for the family members during face-to-face visitation (Christian et al., 2006; McKay, 2016). Moreover, difficulties are present in navigating the prison system and institutional bureaucracies (Christian et al., 2006). The absence of the parent at home potentially entails losing another source of income at home, putting them under further financial strain (Christian et al., 2006; Marković, 2020).

In contrast to face-to-face visitation, video visitation removes the geographical distance, reduces spending and alleviates safety concerns, and simultaneously strengthens familial connections and preserves the family units (Fulcher, 2013; McKay, 2016; Stickel, et al., 2021). Concerning parent-children contact, video visitation may be especially relevant and optimal in providing a supportive and safe environment for relationship growth and psychological well-being (Cramer et al.,

⁶ Rulebook on treatment, treatment program, classification and subsequent classification of convicted persons, Official Gazette RS, No. 66/15.

2017; Stickel, et al., 2021). Some of the reasons may be that face-to-face visitation can aggravate the stress, shame and incompetence of the parent, as well as (re) traumatize the children, e.g. enduring invasive search procedures or prohibiting the physical contact (Cramer et al. 2017; Poehlmann-Tynan & Pritzl, 2019). Although not all factors have been researched, it has been suggested that video visitation allows greater control of the conditions of contact for offenders (Christian et al., 2006; Stickel, et al., 2021).

Furthermore, from the perspective of the prison employees, participation in video visitation could be used as an effective inmate management tool, since it produced better behavior from inmates, fewer disciplinary infractions in prisons and better outcomes after being released from prison (Crabbe, 2002). Video visitation has the added benefit of preventing one of the main ways that drugs and other contraband items enter the prisons (Christian et al., 2006). It has been suggested that some factors may include support, place to live, and jobs reflecting the social capital aspect (Christian et al., 2006), and that the interaction with the technology can affect dependency and lead to self-responsibility and personal control (McDougall et al., 2017).

From the offender perspective, maintaining family contact provides them with emotional support (e.g. bonding with family and children), as well as material support (e.g. money and packages). Moreover, family remains an important link bridging the inside with the outside world and acting as a safe haven after being released (Christian, 2006).

However, maintaining video visitation contact has its limitations. Some authors point to privacy and confidentiality issues, equipment (audio or video) failure, shorter average visiting time and reduction in personal visits to prisons by family, restrictions of video visitation rights (e.g. sex offenders) and the funding of such venture (Crabbe, 2002; Cramer et al., 2017; McKay, 2016; Stickel et al., 2021). Moreover, overcoming the physical distance and financial hardships and improving the permeability to the outside world tends to produce a certain degree of disconnection in some individuals (McKay, 2016), and it is advised against the elimination of physical visitation since it removes certain human contact with the family members (Fulcher, 2013).

2. GOAL AND QUESTIONS

The present study aimed to elucidate the process of contact between incarcerated people and their families and children in the digital environment as seen from the perspective of the prison employees of the PCI Sremska Mitrovica. The study used a qualitative approach that was focused on examining the verbal descrip-

tions provided by the prison employees on the topic of the digital environment in the prison. Specifically, the questions targeted the process of requesting the video conferencing in the prison, when it was introduced, what are the benefits and/or the negative side effects, as well as the effects such digital contact with the family and children has on the treatment and postpenal resocialization of the offenders.

3. METHOD

3.1. Context of the study

The study focused on the characteristics of the digital environment, as well as the contact between the offenders and their families and children, in the PCI Sremska Mitrovica. The study was conducted within the aims of international conference in Palić called “Children and the challenges of digital environment”. In particular, we focused on exploring the capacities of modern technologies in the context of improving living conditions and treatment content in penitentiary institutions, but also in the context of maintaining and improving the quality of family ties, whether the separation of family members is caused by deprivation of liberty of parents and/or children.

A case study research design was used to explore the communication between offenders and their families. The case study method allows the respondents to answer in an open-ended manner, using their own terminology and to discuss their perceptions more fully. The qualitative method of research is particularly appropriate when ‘how’ and ‘why’ questions are being asked of a real-life situation, with the aim of exploration (Bogdanović, 1993).

PCI Sremska Mitrovica was chosen as the largest, most equipped penitentiary, where it was assumed that the research phenomenon has been most represented. Permission to conduct the interviews was granted by the PCI Sremska Mitrovica, and was conducted as one instance within the broader frame of the PrisonLIFE project funded by the Science Fund of the Republic of Serbia.

3.2. Sample and data collection

The invitation to participate was sent to PCI Sremska Mitrovica. The invitation consisted of the aim of the study together with the request for the prison employees to act in the capacity of participants. The sample consisted of three prison employees, with the positions of Deputy Warden, Head of Treatment Services as well as a Treatment Officer. The choice of the participants was guided by the dif-

ferent levels occupied in the workplace and the tasks they perform within their jobs, making them the most relevant informants in the context of video visitation.

All of the interviews occurred on the prison premises, and were conducted in person in the April of 2022. The interviews lasted on average 42 minutes. Informed consent was obtained from all of the participants. Participation was on a voluntary basis, with the right to withdraw from the interview at any time. The participants were also informed about the research aims and the study's content.

3.3. Instrument

The study utilized qualitative in-depth, semi-structured, interviews. The choice of the interview method was guided by the need for detailed information from the field as well as the exploration of new issues in-depth, while simultaneously remaining flexible for the participants and allowing for open-ended discussion. Each participant was asked a total of 9 questions about the contact between offenders and their families and children in the digital environment. The questions related to the following groups: the process of requesting the video link in the prison, both positive and negative sides of the digital environment for the offenders, employees and the institution, and the effects of employing the digital technology with the aim to connect the offenders with their family and children. The prison employees were asked about their experiences and expectations relating to the digital environments program, the thoughts they were having on the process and the outcomes as well as some positive and negative byproducts of using video visitation.

3.4. Analysis

The data, consisting of the statements and commentaries, were analyzed following the qualitative research practices (Bogdanović, 1993). The participants offered their perceptions of the digital environment in prisons from their perspective and of the institutions, as well as those thought held by the offenders.

4. FINDINGS AND DISCUSSION

The study aimed at exploring the video visitation processes in the context of offender-family relationship, with a special focus on children, in PCI Sremska Mitrovica, as seen from the prison employees. The focus was placed on the processes surrounding video visitation as well as on the factors participating in a successful

adjustment in prisons as well as in the reintegration into the community upon release and preventing recidivism.

4.1. The process surrounding digital communication

The procedure requires several steps to be taken before the video visitation could be approved. The first step requires the offender to apply for the visitation to their correctional official, while the final step in the approval process is completed by the Prison Warden. To establish contact with the family through digital means, a specific report is drawn up for the offender who applies.

This report contains the following data about offender: the duration of the sentence; expiration of the sentence; treatment group; extended rights they enjoy; work engagement within the institution; information on the last disciplinary punishment (if any); does he use visits; who comes to visit him; information on whether the person they want to contact is entered in the visit card; as well as information on whether the offender has already made video visitation in the month for which he is seeking approval. The report is then signed by the treatment officer, after which the five-member commission (treatment service, security service, health service, training and employment service and legal affairs service) decides on the submitted application. The decision on the submitted request is signed by the prison warden. Although the deadline for making a decision is 5 days from the day of applying, in practice the decision is usually made within two days. The request can be made by all offenders, regardless of the type of ward and the treatment group in which they are assigned.

The form of the report is not prescribed by the law or any relevant regulations, but was designed in the PCI Sremska Mitrovica. The interviewed employees felt that the invention and introduction of the report form was an indispensable tool in the process of approving requests for video visitation. Such transitional solutions point to examples of good practices and offer a sustainable alternative, until the possibility of the (similar) report is introduced by law, after which this form could be standardized at the level of all prison systems in the country.

Duration of the particular video visitation is limited to 15 minutes per individual offender, once a month. The priority is given to those offenders who are in a difficult position to be physically visited by their family and relatives (e.g. due to the great distance between the prison and the family's place of residence; if the convict's family lives abroad, etc.). Primarily, this type of communication was first introduced for this group of convicts.

Compared to the possibilities currently provided by the Law, in terms of duration, it could be said that video calls are limited in time in the same way as tele-

phone conversations. However, a big difference is noticeable in terms of the frequency of using this type of communication. Thus, telephone calls can be made four times a week (in the case of persons classified in the closed ward) or every day (in the case of persons classified in the semi-open and open ward).

Compared to the right to receive visits, there is uniformity in that both face-to-face visits and video calls are provided only once a month (except in the case of granting extended rights and privileges to receive visits, when the convicted person acquires the opportunity to receive one more visit). However, here is the difference in duration, where face-to-face visits last four times longer than a video call.

Prison infrastructure and architecture. During our fieldwork, we had the opportunity to observe the physical space where the video visitations are taking place. There exists a separate conversation room equipped with a modern system for video communication. The room is located within the new facility in the prison, with a space that allows the privacy of the offender who in this way makes contact with the family. This room is also used in parole proceedings that the PCI Sremska Mitrovica realizes with the Higher Court in Sremska Mitrovica, and recently with the higher court in the Novi Sad. Additionally, the OSCE mission in Serbia donated three tablets, which the correctional officers in the prison system offer to convicts on the basis of approval. These tablets are primarily used in the closed ward of the prison.

It may be noteworthy to indicate the dignified ambience which allows for both privacy and confidentiality. The room also features the modernized equipment reducing the chances for equipment failure. Such ambience prevents or reduces the issues raised with this mode of visitation in previous research (Crabbe, 2002; Cramer et al., 2017; McKay, 2016; Stickel et al., 2021).

4.2. The effect on the offender behavior and the prison employees

Making contact with family and children had become especially important in situations when it was impossible to achieve physical presence. COVID-19 pandemic temporarily prevented the right to face-to-face visits. The digitized type of connection, video visitation, enabled the convicts to make some contact with their families, and especially with their children (Dallaire, 2021; Stickel et al., 2021). The pandemic did not only expose the limiting factors for moving forward, but also presented a viable opportunity. This unprecedented change seemed to have been welcomed by the PCI Sremska Mitrovica. As far as the participants report, they were the first institution to move in this direction, even after the lifting of COVID-19 restrictions. According to their information, the same practice was started

in the PCI for women in Požarevac. Upravo, COVID-19 pandemics je dovela do toga da se video pozivi omoguće i onoj grupi osuđenih lica koja inače ostvaruju pravo na prijem poseta face to face.

From the perspective of the prison employees, all three participants strongly felt that video visitation has been an effective management tool. Since this is at the moment a privilege, it encourages the offender to accept the rules of treatment. The participants also add that there are further positive effects on the relationship between prison employees and offenders. This is in accordance with previous research findings on better behavior from offenders in treatment with fewer disciplinary infractions in prisons and better outcomes after being released from prison (Crabbe, 2002). Two participants further agreed that video visitation improves self-responsibility and personal control (Mcdougall et al., 2017). And although shorter visitation time in video communication was used (McKay, 2016; Stickel et al., 2021), participants feel that exactly is what makes it a privilege and an effective management tool.

Most importantly, all participants strongly felt that the maintenance of strong ties to the families and children is one of the key factors contributing to successful resocialization and post-penal acceptance. Video visitation allows the removal of the geographical distance and builds a more sustaining and lasting image of the parent. This not only allows for a more supportive and safe environment, but also for the possibility to nurture psychological trust as the prerequisite for stable relating (Drndarević & Protić, 2020). This was especially true in the case of children. Elimination of the potential shame and discomfort (Cramer et al., 2017), while enabling the connection was singled out by the majority of the participants. The practical experience of the participants agreed with the previous studies on the importance and usefulness of video visitation in connecting the families (Fulcher, 2013; McKay, 2016; Stickel, et al., 2021).

Concerning the negatives sides, none were perceived and reported by the prison employees in the interviews. Nonetheless, it should be taken into account that the video visitation should not be a complete replacement for the face-to-face visitation, but rather used as a complementary channel (Fulcher, 2013).

4.3. Limitations and future directions

There were limitations to these findings which were mostly due to sampling method and interview approach. The first limitation concerns proneness to bias inherent in the interviewing method, and especially in the sample consisting of the employees of the prison. To minimize the bias and gain a more complete picture, this issue should be examined from the perspective of the offenders. Moreo-

ver, offender perspective would offer the chance to illuminate the potential factors contributing to stronger familial ties – e.g. who is visiting, type of crime, criminal history and so on (Christian et al., 2006). The second limitation relates to non generalizability, once more inherent in the small samples and the absence of random sampling. Considering that the researched topic was not too complex, the same themes were repeatedly uncovered in all three respondents on various institutional levels, indicating that the sufficient sample was reached. Future research would benefit from extending the method to more quantitative methods.

5. CONCLUSION

Introducing the digital technology in a security-tight and highly controlled environment poses new challenges for both the prison systems and the individual rights. But it is justified if the security measures can be met and empirical findings of recidivism rates are favorable. Relevancy of the findings point to good practices examples of introducing video visitation. To the best knowledge of the authors, this was one of the first studies to examine video visitation in Serbian prison systems.

Maintaining contact with the family is undoubtedly one of the most important elements in terms of preparation for the release of a convicted person from serving a prison sentence. The digital environment could be exploited in a similar way as it was decades ago when the possibility of using telephones for similar purposes was introduced, where it seems that greater benefits can come from video calls, since at the same time the convict can not only hear, but also can see his family members. This problem is especially pronounced among those persons who have been sentenced to many years in prison, and who have small children. It is very important that children maintain contact with a parent who is serving a prison sentence, and video technology can be an adequate addition to standard visits.

Our research has shown that video technology in a prison environment gives positive results. The practice carried out by the PCI Sremska Mitrovica is an example of good treatment, i.e. a practice that is increasingly present in modern systems of execution of criminal sanctions, but also a standard established by Mandela's rules. For this reason, this type of treatment should be supported, but further developed, bearing in mind that this matter needs to be included in the legal framework, in order to enable video calls to be made by all convicted person, not just those who support sentence in the PCI Sremska Mitrovica.

It is our opinion that the use of video technologies can't be a substitute, but only a supplement to the already existing rights and / or extended rights and

privileges of the convicted person. An analogy with telephone calls would imply that this is a general right that belongs to every convicted person, while the question remains to what extent it would be possible, i.e. how many times a week / month, as well as its duration. An analogy with extended rights and privileges would mean that convicted persons must first fulfill an appropriate program of treatment, that is, a video call would be a benefit rather than a right that belongs to every convict. At this moment, the second option seems to be a better solution, as it could influence the convict to accept the treatment program. Since we see this as a benefit granted and used within the prison, it could be obtained by all convicted persons who behave particularly well and tries hard and achieves progress against the sentence program (regardless of the prison ward and treatment group). Amendments of the Law must be accompanied by amendments of secondary regulations, primarily the House Rules and the Rulebook of Treatment. It should be borne in mind that the introduction of this possibility must be accompanied by good information systems within the prisons, i.e. the provision of a sufficient number of computers, tablets or other similar devices, which necessarily requires additional funding. Finally, we emphasize once again that video technologies cannot be a substitute for receiving visits, but only their supplement, which is also the case with phone calls.

REFERENCES

1. Bogdanović, M (1993) *Metodološke studije*. Beograd: Institut za političke studije.
2. Bugarski, T. (2021) Preduzimanje procesnih radnji putem tehničkih sredstava u krivičnim stvarima. In: Bejatović, S. (ed.) *Videolink i druga tehnička sredstva kao načini preduzimanja procesnih radnji u kaznenom postupku (norma, praksa i poželjni slučajevi širenja mogućnosti primene)*. Beograd: Misija OEBS-a u Srbiji, pp. 79-94.
3. Christian, J., Mellow, J., & Thomas, S. (2006). Social and economic implications of family connections to prisoners. *Journal of Criminal Justice*, 34(4), pp. 443-452.
4. Coyle, A. (2008) The treatment of prisoners: International standards and case law, *Legal and Criminological Psychology*, 13, pp. 219-230.
5. Crabbe, M. (2002) Virtual visitation program uses video conferencing to strengthen prisoner contacts with families and children. *Offender Programs Report*, 6(3), pp. 35-47.

6. Cramer, L., Goff, M., Peterson, B., & Sandstrom, H. (2017) Parent-child visiting practices in prisons and jails. Washington: Urban Institute.
7. Dallaire, D. H., Shlafer, R. J., Goshin, L. S., Hollihan, A., Poehlmann-Tynan, J., Eddy, J. M., & Adalist-Estrin, A. (2021) COVID-19 and prison policies related to communication with family members. *Psychology, Public Policy, and Law*, 27(2), pp. 231-241.
8. Drndarević, N. & Protić, S. (2020) Analysis of Trust in Serbia: Psychological and Sociological Implications. *Zbornik instituta za kriminološka i sociološka istraživanja*, 39(1), pp. 7-25.
9. Fulcher, P. A. (2013) The double-edged sword of prison video visitation: Claiming to keep families together while furthering the aims of the prison industrial complex. *Fla. A & M UL Rev.*, 9(1), pp. 83-112.
10. Järveläinen, E., & Rantanen, T. (2021) Incarcerated people's challenges for digital inclusion in Finnish prisons. *Nordic Journal of Criminology*, 22(2), pp. 240-259.
11. Kubiček, A., Batrićević, A., & Paraušić, A. (2020) Prison Based Educational Programs as a Means to Promote Ex-prisoners' Right to Labour. In: Ilik, G. & Stojanoska, A. (ed.) *Towards a Better Future: Human Rights, Organized Crime and Digital Society*. Bitola: Center for Scientific Research at the Faculty of Law.
12. Law on Execution of Criminal Sanctions, Official Gazette RS, No. 55/14 & 35/19.
13. Marković, A. (2020) Prekarijat i neka pitanja društvene strukture i društvenih nejednakosti. *Zbornik instituta za kriminološka i sociološka istraživanja*, 39(2-3), pp. 109-126.
14. McDougall, C., Pearson, D. A., Torgerson, D. J., & Garcia-Reyes, M. (2017) The effect of digital technology on prisoner behavior and reoffending: a natural stepped-wedge design. *Journal of Experimental Criminology*, 13(4), 455-482.
15. McKay, C. (2016) Video links from prison: Permeability and the carceral world. *International Journal for Crime, Justice and Social Democracy*, 5(1), pp. 21-37.
16. Miljuš, I. (2021) Upotreba tehničkih sredstava za prenos slike i zvuka i pravo na pravično suđenje. In: Bejatović, S. (ed.) *Videolink i druga tehnička sredstva kao načini preduzimanja procesnih radnji u kaznenom postupku (norma, praksa i poželjni slučajevi širenja mogućnosti primene)*. Beograd: Misija OEBS-a u Srbiji, pp. 227-248.

17. Poehlmann-Tynan, J., & Pritzl, K. (2019) Parent–child visits when parents are incarcerated in prison or jail. In: *Handbook on children with incarcerated parents*. Cham: Springer, pp. 131-147.
18. Powell, A., Stratton, G., & Cameron, R. (2018) *Digital criminology: Crime and justice in digital society*. Abingdon: Routledge.
19. Rulebook of the house rules of penitentiary institutions and district prisons, Official Gazette RS, No. 110/14 & 79/16.
20. Rulebook on treatment, treatment program, classification and subsequent classification of convicted persons, Official Gazette RS, No. 66/15.
21. Stickel, T., Prins, E., & Kaiper-Marquez, A. (2021) ‘The video is an upgrade from them all’: how incarcerated fathers view the affordances of video in a family literacy programme. *Learning, Media and Technology*, 46(2), pp. 174-189.

Nikola Vujičić, MA

Istraživač saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

Nikola Drndarević, MA

Istraživač pripravnik, Institut za kriminološka i sociološka istraživanja u Beogradu

OSUĐENICI I NJIHOVE PORODICE U DIGITALNOM OKRUŽENJU: STUDIJA SLUČAJA U KPZ SREMSKA MITROVICA⁷

U radu je dat prikaz razvoja i osnovnih karakteristika “video poseta” u Kazneno-popravnom zavodu u Sremskoj Mitrovici, sa posebnim fokusom na kontakt između osuđenika i njihovih porodica. Studija je zasnovana na podacima koji su dobijeni na osnovu intervjua sprovedenih sa zaposlenima u navedenom zavodu, sa ciljem da se sagledaju iskustva upotrebe video linka kao načina ostvarivanja poseta, te njihov značaj na ponašanje osuđenika tokom izdržavanja kazne zatvora. Takođe, u radu su analizirani stavovi stručnjaka, odnosno onih lica koja direktno rade sa osuđenima, u kontekstu uticaja video poziva na održavanje kontakta sa porodicama. Priroda digitalnog okruženja u zatvorskom sistemu, posebno je sagledana i sa aspekta norme, odnosno zakonodavnog okvira u Republici Srbiji.

KLJUČNE REČI: zatvori / digitalno okruženje / video posete / kontakt sa porodicom / deca

⁷ Istraživanje je sprovedeno uz podršku Fonda za nauku, broj Projekta: 7750249, naziv: Assessment and possibilities for improving the quality of prison life of prisoners in the Republic of Serbia: Criminological-Penological, Psychological, Sociological, Legal and Security Aspects (PrisonLIFE)

ANNEXES



Convention on the Rights of the Child

Distr.: General
2 March 2021

Original: English

Committee on the Rights of the Child

General comment No. 25 (2021) on children's rights in relation to the digital environment

I. Introduction

1. The children consulted for the present general comment reported that digital technologies were vital to their current lives and to their future: "By the means of digital technology, we can get information from all around the world"; "[Digital technology] introduced me to major aspects of how I identify myself"; "When you are sad, the Internet can help you [to] see something that brings you joy".¹

2. The digital environment is constantly evolving and expanding, encompassing information and communications technologies, including digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology.²

3. The digital environment is becoming increasingly important across most aspects of children's lives, including during times of crisis, as societal functions, including education, government services and commerce, progressively come to rely upon digital technologies. It affords new opportunities for the realization of children's rights, but also poses the risks of their violation or abuse. During consultations, children expressed the view that the digital environment should support, promote and protect their safe and equitable engagement: "We would like the government, technology companies and teachers to help us [to] manage untrustworthy information online."; "I would like to obtain clarity about what really happens with my data ... Why collect it? How is it being collected?"; "I am ... worried about my data being shared".³

4. The rights of every child must be respected, protected and fulfilled in the digital environment. Innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the Internet. Meaningful access to digital technologies can support children to realize the full range of their civil, political, cultural, economic and social rights. However, if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise.

5. The present general comment draws on the Committee's experience in reviewing States parties' reports, its day of general discussion on digital media and children's rights, the jurisprudence of the human rights treaty bodies, the recommendations of the Human

¹ "Our rights in a digital world", summary report on the consultation of children for the present general comment, pp. 14 and 22. Available from <https://5rightsfoundation.com/uploads/Our%20Rights%20in%20a%20Digital%20World.pdf>. All references to children's views refer to that report.

² A terminology glossary is available on the Committee's webpage: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCRC%2fINF%2f9314&Lang=en.

³ "Our rights in a digital world", pp. 14, 16, 22 and 25.



Rights Council and the special procedures of the Council, two rounds of consultations with States, experts and other stakeholders on the concept note and advanced draft and an international consultation with 709 children living in a wide variety of circumstances in 28 countries in several regions.

6. The present general comment should be read in conjunction with other relevant general comments of the Committee and its guidelines regarding the implementation of the Optional Protocol to the Convention on the sale of children, child prostitution and child pornography.

II. Objective

7. In the present general comment, the Committee explains how States parties should implement the Convention in relation to the digital environment and provides guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and the Optional Protocols thereto in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment.

III. General principles

8. The following four principles provide a lens through which the implementation of all other rights under the Convention should be viewed. They should serve as a guide for determining the measures needed to guarantee the realization of children's rights in relation to the digital environment.

A. Non-discrimination

9. The right to non-discrimination requires that States parties ensure that all children have equal and effective access to the digital environment in ways that are meaningful for them.⁴ States parties should take all measures necessary to overcome digital exclusion. That includes providing free and safe access for children in dedicated public locations and investing in policies and programmes that support all children's affordable access to, and knowledgeable use of, digital technologies in educational settings, communities and homes.

10. Children may be discriminated against by their being excluded from using digital technologies and services or by receiving hateful communications or unfair treatment through use of those technologies. Other forms of discrimination can arise when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child.

11. The Committee calls upon States parties to take proactive measures to prevent discrimination on the basis of sex, disability, socioeconomic background, ethnic or national origin, language or any other grounds, and discrimination against minority and indigenous children, asylum-seeking, refugee and migrant children, lesbian, gay, bisexual, transgender and intersex children, children who are victims and survivors of trafficking or sexual exploitation, children in alternative care, children deprived of liberty and children in other vulnerable situations. Specific measures will be required to close the gender-related digital divide for girls and to ensure that particular attention is given to access, digital literacy, privacy and online safety.

B. Best interests of the child

12. The best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context.⁵ The digital environment was not originally designed for

⁴ General comment No. 9 (2006), paras. 37–38.

⁵ General comment No. 14 (2013), para. 1.

children, yet it plays a significant role in children's lives. States parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration.

13. States parties should involve the national and local bodies that oversee the fulfilment of the rights of children in such actions. In considering the best interests of the child, they should have regard for all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, and ensure transparency in the assessment of the best interests of the child and the criteria that have been applied.

C. Right to life, survival and development

14. Opportunities provided by the digital environment play an increasingly crucial role in children's development and may be vital for children's life and survival, especially in situations of crisis. States parties should take all appropriate measures to protect children from risks to their right to life, survival and development. Risks relating to content, contact, conduct and contract encompass, among other things, violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist. States parties should identify and address the emerging risks that children face in diverse contexts, including by listening to their views on the nature of the particular risks that they face.

15. The use of digital devices should not be harmful, nor should it be a substitute for in-person interactions among children or between children and parents or caregivers. States parties should pay specific attention to the effects of technology in the earliest years of life, when brain plasticity is maximal and the social environment, in particular relationships with parents and caregivers, is crucial to shaping children's cognitive, emotional and social development. In the early years, precautions may be required, depending on the design, purpose and uses of technologies. Training and advice on the appropriate use of digital devices should be given to parents, caregivers, educators and other relevant actors, taking into account the research on the effects of digital technologies on children's development, especially during the critical neurological growth spurts of early childhood and adolescence.⁶

D. Respect for the views of the child

16. Children reported that the digital environment afforded them crucial opportunities for their voices to be heard in matters that affected them.⁷ The use of digital technologies can help to realize children's participation at the local, national and international levels.⁸ States parties should promote awareness of, and access to, digital means for children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed, so that they can be effective advocates for their rights, individually and as a group.

17. When developing legislation, policies, programmes, services and training on children's rights in relation to the digital environment, States parties should involve all children, listen to their needs and give due weight to their views. They should ensure that digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services.

18. States parties are encouraged to utilize the digital environment to consult with children on relevant legislative, administrative and other measures and to ensure that their views are considered seriously and that children's participation does not result in undue monitoring or data collection that violates their right to privacy, freedom of thought and opinion. They

⁶ General comment No. 24 (2019), para. 22; and general comment No. 20 (2016), paras. 9–11.

⁷ "Our rights in a digital world", p. 17.

⁸ General comment No. 14 (2013), paras. 89–91.

should ensure that consultative processes are inclusive of children who lack access to technology or the skills to use it.

IV. Evolving capacities

19. States parties should respect the evolving capacities of the child as an enabling principle that addresses the process of their gradual acquisition of competencies, understanding and agency.⁹ That process has particular significance in the digital environment, where children can engage more independently from supervision by parents and caregivers. The risks and opportunities associated with children's engagement in the digital environment change depending on their age and stage of development. They should be guided by those considerations whenever they are designing measures to protect children in, or facilitate their access to, that environment. The design of age-appropriate measures should be informed by the best and most up-to-date research available, from a range of disciplines.

20. States parties should take into account the changing position of children and their agency in the modern world, children's competence and understanding, which develop unevenly across areas of skill and activity, and the diverse nature of the risks involved. Those considerations must be balanced with the importance of exercising their rights in supported environments and the range of individual experiences and circumstances.¹⁰ States parties should ensure that digital service providers offer services that are appropriate for children's evolving capacities.

21. In accordance with States' duty to render appropriate assistance to parents and caregivers in the performance of their child-rearing responsibilities, States parties should promote awareness among parents and caregivers of the need to respect children's evolving autonomy, capacities and privacy. They should support parents and caregivers in acquiring digital literacy and awareness of the risks to children in order to help them to assist children in the realization of their rights, including to protection, in relation to the digital environment.

V. General measures of implementation by States parties

22. Opportunities for the realization of children's rights and their protection in the digital environment require a broad range of legislative, administrative and other measures, including precautionary ones.

A. Legislation

23. States parties should review, adopt and update national legislation in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention and the Optional Protocols thereto. Legislation should remain relevant, in the context of technological advances and emerging practices. They should mandate the use of child rights impact assessments to embed children's rights into legislation, budgetary allocations and other administrative decisions relating to the digital environment and promote their use among public bodies and businesses relating to the digital environment.¹¹

B. Comprehensive policy and strategy

24. States parties should ensure that national policies relating to children's rights specifically address the digital environment, and they should implement regulation, industry

⁹ General comment No. 7 (2005), para. 17; and general comment No. 20 (2016), paras. 18 and 20.

¹⁰ General comment No. 20 (2016), para. 20.

¹¹ General comment No. 5 (2003), para. 45; general comment No. 14 (2013), para. 99; and general comment No. 16 (2013), paras. 78–81.

codes, design standards and action plans accordingly, all of which should be regularly evaluated and updated. Such national policies should be aimed at providing children with the opportunity to benefit from engaging with the digital environment and ensuring their safe access to it.

25. Children's online protection should be integrated within national child protection policies. States parties should implement measures that protect children from risks, including cyberaggression and digital technology-facilitated and online child sexual exploitation and abuse, ensure the investigation of such crimes and provide remedy and support for children who are victims. They should also address the needs of children in disadvantaged or vulnerable situations, including by providing child-friendly information that is, when necessary, translated into relevant minority languages.

26. States parties should ensure the operation of effective child protection mechanisms online and safeguarding policies, while also respecting children's other rights, in all settings where children access the digital environment, which includes the home, educational settings, cybercafés, youth centres, libraries and health and alternative care settings.

C. Coordination

27. To encompass the cross-cutting consequences of the digital environment for children's rights, States parties should identify a government body that is mandated to coordinate policies, guidelines and programmes relating to children's rights among central government departments and the various levels of government.¹² Such a national coordination mechanism should engage with schools and the information and communications technology sector and cooperate with businesses, civil society, academia and organizations to realize children's rights in relation to the digital environment at the cross-sectoral, national, regional and local levels.¹³ It should draw on technological and other relevant expertise within and beyond government, as needed, and be independently evaluated for its effectiveness in meeting its obligations.

D. Allocation of resources

28. States parties should mobilize, allocate and utilize public resources to implement legislation, policies and programmes to fully realize children's rights in the digital environment and to improve digital inclusion, which is needed to address the increasing impact of the digital environment on children's lives and to promote the equality of access to, and affordability of, services and connectivity.¹⁴

29. Where resources are contributed from the business sector or obtained through international cooperation, States parties should ensure that their own mandate, revenue mobilization, budget allocations and expenditure are not interfered with or undermined by third parties.¹⁵

E. Data collection and research

30. Regularly updated data and research are crucial to understanding the implications of the digital environment for children's lives, evaluating its impact on their rights and assessing the effectiveness of State interventions. States parties should ensure the collection of robust, comprehensive data that is adequately resourced and that data are disaggregated by age, sex, disability, geographical location, ethnic and national origin and socioeconomic background. Such data and research, including research conducted with and by children, should inform legislation, policy and practice and should be available in the public domain.¹⁶ Data

¹² General comment No. 5 (2003), para. 37.

¹³ *Ibid.*, paras. 27 and 39.

¹⁴ General comment No. 19 (2016), para. 21.

¹⁵ *Ibid.*, para. 27 (b).

¹⁶ General comment No. 5 (2003), paras. 48 and 50.

collection and research relating to children's digital lives must respect their privacy and meet the highest ethical standards.

F. Independent monitoring

31. States parties should ensure that the mandates of national human rights institutions and other appropriate independent institutions cover children's rights in the digital environment and that they are able to receive, investigate and address complaints from children and their representatives.¹⁷ Where independent oversight bodies exist to monitor activities in relation to the digital environment, national human rights institutions should work closely with such bodies on effectively discharging their mandate regarding children's rights.¹⁸

G. Dissemination of information, awareness-raising and training

32. States parties should disseminate information and conduct awareness-raising campaigns on the rights of the child in the digital environment, focusing in particular on those whose actions have a direct or indirect impact on children. They should facilitate educational programmes for children, parents and caregivers, the general public and policymakers to enhance their knowledge of children's rights in relation to the opportunities and risks associated with digital products and services. Such programmes should include information on how children can benefit from digital products and services and develop their digital literacy and skills, how to protect children's privacy and prevent victimization and how to recognize a child who is a victim of harm perpetrated online or offline and respond appropriately. Such programmes should be informed by research and consultations with children, parents and caregivers.

33. Professionals working for and with children and the business sector, including the technology industry, should receive training that includes how the digital environment affects the rights of the child in multiple contexts, the ways in which children exercise their rights in the digital environment and how they access and use technologies. They should also receive training on the application of international human rights standards to the digital environment. States parties should ensure that pre-service and in-service training relating to the digital environment is provided for professionals working at all levels of education, to support the development of their knowledge, skills and practice.

H. Cooperation with civil society

34. States parties should systematically involve civil society, including child-led groups and non-governmental organizations working in the field of children's rights and those concerned with the digital environment, in the development, implementation, monitoring and evaluation of laws, policies, plans and programmes relating to children's rights. They should also ensure that civil society organizations are able to implement their activities relating to the promotion and protection of children's rights in relation to the digital environment.

I. Children's rights and the business sector

35. The business sector, including not-for-profit organizations, affects children's rights directly and indirectly in the provision of services and products relating to the digital environment. Businesses should respect children's rights and prevent and remedy abuse of their rights in relation to the digital environment. States parties have the obligation to ensure that businesses meet those responsibilities.¹⁹

¹⁷ General comment No. 2 (2002), paras. 2 and 7.

¹⁸ *Ibid.*, para. 7.

¹⁹ General comment No. 16 (2013), paras. 28, 42 and 82.

36. States parties should take measures, including through the development, monitoring, implementation and evaluation of legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies. They should also encourage businesses to provide public information and accessible and timely advice to support children's safe and beneficial digital activities.

37. States parties have a duty to protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment. Although businesses may not be directly involved in perpetrating harmful acts, they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services. States parties should put in place, monitor and enforce laws and regulations aimed at preventing violations of the right to protection from violence, as well as those aimed at investigating, adjudicating on and redressing violations as they occur in relation to the digital environment.²⁰

38. States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children.²¹ They should take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses.

39. In addition to developing legislation and policies, States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child. They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service.

J. Commercial advertising and marketing

40. The digital environment includes businesses that rely financially on processing personal data to target revenue-generating or paid-for content, and such processes intentionally and unintentionally affect the digital experiences of children. Many of those processes involve multiple commercial partners, creating a supply chain of commercial activity and the processing of personal data that may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content.

41. States parties should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes.

42. States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products,

²⁰ Ibid., para. 60.

²¹ Ibid., paras. 50 and 62–65.

applications and services should also be prohibited from engagement directly or indirectly with children.

K. Access to justice and remedies

43. Children face particular challenges in access to justice relating to the digital environment for a range of reasons. Such challenges arise because of the lack of legislation placing sanctions on children's rights violations specifically in relation to the digital environment, the difficulties in obtaining evidence or identifying perpetrators or because children and their parents or caregivers lack knowledge of their rights or of what constitutes a violation or abuse of their rights in the digital environment, among other factors. Further challenges may arise if children are required to disclose sensitive or private online activities or from their fear of reprisals by peers or of social exclusion.

44. States parties should ensure that appropriate and effective remedial judicial and non-judicial mechanisms for the violations of children's rights relating to the digital environment are widely known and readily available to all children and their representatives. Complaint and reporting mechanisms should be free of charge, safe, confidential, responsive, child-friendly and available in accessible formats. States parties should also provide for collective complaints, including class action and public interest litigation, and for legal or other appropriate assistance, including through specialized services, to children whose rights have been violated in or through the digital environment.

45. States parties should establish, coordinate and regularly monitor and evaluate frameworks for the referral of such cases and the provision of effective support to children who are victims.²² Frameworks should include measures for the identification of, therapy and follow-up care for, and the social reintegration of, children who are victims. Training on the identification of children who are victims should be included in referral mechanisms, including for digital service providers. Measures within such a framework should be multi-agency and child-friendly, to prevent a child's revictimization and secondary victimization in the context of investigative and judicial processes. That may require specialized protections for confidentiality and to redress harms associated with the digital environment.

46. Appropriate reparation includes restitution, compensation and satisfaction and may require apology, correction, removal of unlawful content, access to psychological recovery services or other measures.²³ In relation to violations in the digital environment, remedial mechanisms should take into account the vulnerability of children and the need to be swift to halt ongoing and future damage. States parties should guarantee the non-recurrence of violations, including by the reform of relevant laws and policies and their effective implementation.

47. Digital technologies bring additional complexity to the investigation and prosecution of crimes against children, which may cross national borders. States parties should address the ways in which uses of digital technologies may facilitate or impede the investigation and prosecution of crimes against children and take all available preventative, enforcement and remedial measures, including in cooperation with international partners. They should provide specialized training for law enforcement officials, prosecutors and judges regarding child rights violations specifically associated with the digital environment, including through international cooperation.

48. Children may face particular difficulties in obtaining remedy when their rights have been abused in the digital environment by business enterprises, in particular in the context of their global operations.²⁴ States parties should consider measures to respect, protect and fulfil children's rights in the context of businesses' extraterritorial activities and operations, provided that there is a reasonable link between the State and the conduct concerned. They should ensure that businesses provide effective complaint mechanisms; such mechanisms should not, however, prevent children from gaining access to State-based remedies. They

²² General comment No. 21 (2017), para. 22. See also General Assembly resolution 60/147, annex.

²³ General comment No. 5 (2003), para. 24.

²⁴ General comment No. 16 (2013), paras. 66–67.

should also ensure that agencies with oversight powers relevant to children's rights, such as those relating to health and safety, data protection and consumer rights, education and advertising and marketing, investigate complaints and provide adequate remedies for violations or abuses of children's rights in the digital environment.²⁵

49. States parties should provide children with child-sensitive and age-appropriate information in child-friendly language on their rights and on the reporting and complaint mechanisms, services and remedies available to them in cases where their rights in relation to the digital environment are violated or abused. Such information should also be provided to parents, caregivers and professionals working with and for children.

VI. Civil rights and freedoms

A. Access to information

50. The digital environment provides a unique opportunity for children to realize the right to access to information. In that regard, information and communications media, including digital and online content, perform an important function.²⁶ States parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary for the purposes stipulated in article 13 of the Convention.

51. States parties should provide and support the creation of age-appropriate and empowering digital content for children in accordance with children's evolving capacities and ensure that children have access to a wide diversity of information, including information held by public bodies, about culture, sports, the arts, health, civil and political affairs and children's rights.

52. States parties should encourage the production and dissemination of such content using multiple formats and from a plurality of national and international sources, including news media, broadcasters, museums, libraries and educational, scientific and cultural organizations. They should particularly endeavour to enhance the provision of diverse, accessible and beneficial content for children with disabilities and children belonging to ethnic, linguistic, indigenous and other minority groups. The ability to access relevant information, in the languages that children understand, can have a significant positive impact on equality.²⁷

53. States parties should ensure that all children are informed about, and can easily find, diverse and good quality information online, including content independent of commercial or political interests. They should ensure that automated search and information filtering, including recommendation systems, do not prioritize paid content with a commercial or political motivation over children's choices or at the cost of children's right to information.

54. The digital environment can include gender-stereotyped, discriminatory, racist, violent, pornographic and exploitative information, as well as false narratives, misinformation and disinformation and information encouraging children to engage in unlawful or harmful activities. Such information may come from multiple sources, including other users, commercial content creators, sexual offenders or armed groups designated as terrorist or violent extremist. States parties should protect children from harmful and untrustworthy content and ensure that relevant businesses and other providers of digital content develop and implement guidelines to enable children to safely access diverse content, recognizing children's rights to information and freedom of expression, while protecting them from such harmful material in accordance with their rights and evolving capacities.²⁸ Any restrictions on the operation of any Internet-based, electronic or other information

²⁵ Ibid., paras. 30 and 43.

²⁶ General comment No. 7 (2005), para. 35; and general comment No. 20 (2016), para. 47.

²⁷ General comment No. 17 (2013), para. 46; and general comment No. 20 (2016), paras. 47–48.

²⁸ General comment No. 16 (2013), para. 58; and general comment No. 7 (2005), para. 35.

dissemination systems should be in line with article 13 of the Convention.²⁹ States parties should not intentionally obstruct or enable other actors to obstruct the supply of electricity, cellular networks or Internet connectivity in any geographical area, whether in part or as a whole, which can have the effect of hindering a child's access to information and communication.

55. States parties should encourage providers of digital services used by children to apply concise and intelligible content labelling, for example on the age-appropriateness or trustworthiness of content. They should also encourage the provision of accessible guidance, training, educational materials and reporting mechanisms for children, parents and caregivers, educators and relevant professional groups.³⁰ Age-based or content-based systems designed to protect children from age-inappropriate content should be consistent with the principle of data minimization.

56. States parties should ensure that digital service providers comply with relevant guidelines, standards and codes³¹ and enforce lawful, necessary and proportionate content moderation rules. Content controls, school filtering systems and other safety-oriented technologies should not be used to restrict children's access to information in the digital environment; they should be used only to prevent the flow of harmful material to children. Content moderation and content controls should be balanced with the right to protection against violations of children's other rights, notably their rights to freedom of expression and privacy.

57. Professional codes of conduct set by news media and other relevant organizations should include guidance on how to report digital risks and opportunities relating to children. Such guidance should result in evidence-based reporting that does not reveal the identity of children who are victims and survivors and that is in accordance with international human rights standards.

B. Freedom of expression

58. Children's right to freedom of expression includes the freedom to seek, receive and impart information and ideas of all kinds, using any media of their choice. Children reported³² that the digital environment offered significant scope to express their ideas, opinions and political views. For children in disadvantaged or vulnerable situations, technology-facilitated interaction with others who share their experiences can help them to express themselves.

59. Any restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate. The rationale for such restrictions should be transparent and communicated to children in age-appropriate language. States parties should provide children with information and training opportunities on how to effectively exercise that right, in particular how to create and share digital content safely, while respecting the rights and dignity of others and not violating legislation, such as that relating to incitement to hatred and violence.

60. When children express their political or other views and identities in the digital environment, they may attract criticism, hostility, threats or punishment. States parties should protect children from cyberaggression and threats, censorship, data breaches and digital surveillance. Children should not be prosecuted for expressing their opinions in the digital environment, unless they violate restrictions provided by criminal legislation which are compatible with article 13 of the Convention.

61. Given the existence of commercial and political motivations to promote particular world views, States parties should ensure that uses of automated processes of information filtering, profiling, marketing and decision-making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment.

²⁹ Human Rights Committee, general comment No. 34 (2011), para. 43.

³⁰ General comment No. 16 (2013), paras. 19 and 59.

³¹ *Ibid.*, paras. 58 and 61.

³² "Our rights in a digital world", p. 16.

C. Freedom of thought, conscience and religion

62. States parties should respect the right of the child to freedom of thought, conscience and religion in the digital environment. The Committee encourages States parties to introduce or update data protection regulation and design standards that identify, define and prohibit practices that manipulate or interfere with children's right to freedom of thought and belief in the digital environment, for example by emotional analytics or inference. Automated systems may be used to make inferences about a child's inner state. They should ensure that automated systems or information filtering systems are not used to affect or influence children's behaviour or emotions or to limit their opportunities or development.

63. States parties should ensure that children are not penalized for their religion or beliefs or have their future opportunities in any other way restricted. The exercise of children's right to manifest their religion or beliefs in the digital environment may be subject only to limitations that are lawful, necessary and proportionate.

D. Freedom of association and peaceful assembly

64. The digital environment can enable children to form their social, religious, cultural, ethnic, sexual and political identities and to participate in associated communities and in public spaces for deliberation, cultural exchange, social cohesion and diversity.³³ Children reported that the digital environment provided them with valued opportunities to meet, exchange and deliberate with peers, decision makers and others who shared their interests.³⁴

65. States parties should ensure that their laws, regulations and policies protect children's right to participate in organizations that operate partially or exclusively in the digital environment. No restrictions may be placed on the exercise by children of their right to freedom of association and peaceful assembly in the digital environment other than those that are lawful, necessary and proportionate.³⁵ Such participation should not in and of itself result in negative consequences to those children, such as exclusion from a school, restriction or deprivation of future opportunities or creation of a police profile. Such participation should be safe, private and free from surveillance by public or private entities.

66. Public visibility and networking opportunities in the digital environment can also support child-led activism and can empower children as advocates for human rights. The Committee recognizes that the digital environment enables children, including children human rights defenders, as well as children in vulnerable situations, to communicate with each other, advocate for their rights and form associations. States parties should support them, including by facilitating the creation of specific digital spaces, and ensure their safety.

E. Right to privacy

67. Privacy is vital to children's agency, dignity and safety and for the exercise of their rights. Children's personal data are processed to offer educational, health and other benefits to them. Threats to children's privacy may arise from data collection and processing by public institutions, businesses and other organizations, as well as from such criminal activities as identity theft. Threats may also arise from children's own activities and from the activities of family members, peers or others, for example, by parents sharing photographs online or a stranger sharing information about a child.

68. Data may include information about, inter alia, children's identities, activities, location, communication, emotions, health and relationships. Certain combinations of personal data, including biometric data, can uniquely identify a child. Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy; they may have

³³ General comment No. 17 (2013), para. 21; and general comment No. 20 (2016), paras. 44–45.

³⁴ "Our rights in a digital world", p. 20.

³⁵ Human Rights Committee, general comment No. 37 (2020), paras. 6 and 34.

adverse consequences on children, which can continue to affect them at later stages of their lives.

69. Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention.

70. States parties should take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Legislation should include strong safeguards, transparency, independent oversight and access to remedy. States parties should require the integration of privacy-by-design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. Where encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. Such measures must be strictly limited according to the principles of legality, necessity and proportionality.

71. Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver.

72. States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations.³⁶ They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats.

73. Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures.³⁷ Children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child, parent or caregiver, as appropriate.

74. Privacy and data protection legislation and measures should not arbitrarily limit children's other rights, such as their right to freedom of expression or protection. States parties should ensure that data protection legislation respects children's privacy and personal data in relation to the digital environment. Through continual technological innovation, the scope of the digital environment is expanding to include ever more services and products, such as clothes and toys. As settings where children spend time become "connected", through the use of embedded sensors connected to automated systems, States parties should ensure that the products and services that contribute to such environments are subject to robust data protection and other privacy regulations and standards. That includes public settings, such as

³⁶ Human Rights Committee, general comment No. 16 (1988), para. 10.

³⁷ *Ibid.*; and Committee on the Rights of the Child, general comment No. 20 (2016), para. 46.

streets, schools, libraries, sports and entertainment venues and business premises, including shops and cinemas, and the home.

75. Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose.

76. The digital environment presents particular problems for parents and caregivers in respecting children's right to privacy. Technologies that monitor online activities for safety purposes, such as tracking devices and services, if not implemented carefully, may prevent a child from accessing a helpline or searching for sensitive information. States parties should advise children, parents and caregivers and the public on the importance of the child's right to privacy and on how their own practices may threaten that right. They should also be advised about the practices through which they can respect and protect children's privacy in relation to the digital environment, while keeping them safe. Parents' and caregivers' monitoring of a child's digital activity should be proportionate and in accordance with the child's evolving capacities.

77. Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should require an approach integrating safety-by-design and privacy-by-design to anonymity, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyberaggression, hate speech or sexual exploitation and abuse. Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care. Such cases may require further intervention, as well as family counselling or other services, to safeguard the child's right to privacy.

78. Providers of preventive or counselling services to children in the digital environment should be exempt from any requirement for a child user to obtain parental consent in order to access such services.³⁸ Such services should be held to high standards of privacy and child protection.

F. Birth registration and right to identity

79. States parties should promote the use of digital identification systems that enable all newborn children to have their birth registered and officially recognized by the national authorities, in order to facilitate access to services, including health, education and welfare. Lack of birth registration facilitates the violation of children's rights under the Convention and the Optional Protocols thereto. States parties should use up-to-date technology, including mobile registration units, to ensure access to birth registration, especially for children in remote areas, refugee and migrant children, children at risk and those in marginalized situations, and include children born prior to the introduction of digital identification systems. For such systems to benefit children, they should conduct awareness-raising campaigns, establish monitoring mechanisms, promote community engagement and ensure effective coordination between different actors, including civil status officers, judges, notaries, health officials and child protection agency personnel. They should also ensure that a robust privacy and data protection framework is in place.

VII. Violence against children

80. The digital environment may open up new ways to perpetrate violence against children, by facilitating situations in which children experience violence and/or may be

³⁸ General comment No. 20 (2016), para. 60.

influenced to do harm to themselves or others. Crises, such as pandemics, may lead to an increased risk of harm online, given that children spend more time on virtual platforms in those circumstances.

81. Sexual offenders may use digital technologies to solicit children for sexual purposes and to participate in online child sexual abuse, for example, by the live video streaming, production and distribution of child sexual abuse material and through sexual extortion. Forms of digitally facilitated violence and sexual exploitation and abuse may also be perpetrated within a child's circle of trust, by family or friends or, for adolescents, by intimate partners, and may include cyberaggression, including bullying and threats to reputation, the non-consensual creation or sharing of sexualized text or images, such as self-generated content by solicitation and/or coercion, and the promotion of self-harming behaviours, such as cutting, suicidal behaviour or eating disorders. Where children have carried out such actions, States parties should pursue preventive, safeguarding and restorative justice approaches for the children involved whenever possible.³⁹

82. States parties should take legislative and administrative measures to protect children from violence in the digital environment, including the regular review, updating and enforcement of robust legislative, regulatory and institutional frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment. Such risks include physical or mental violence, injury or abuse, neglect or maltreatment, exploitation and abuse, including sexual exploitation and abuse, child trafficking, gender-based violence, cyberaggression, cyberattacks and information warfare. States parties should implement safety and protective measures in accordance with children's evolving capacities.

83. The digital environment can open up new ways for non-State groups, including armed groups designated as terrorist or violent extremist, to recruit and exploit children to engage with or participate in violence. States parties should ensure that legislation prohibits the recruitment of children by terrorist or violent extremist groups. Children accused of criminal offences in that context should be treated primarily as victims but, if charged, the child justice system should apply.

VIII. Family environment and alternative care

84. Many parents and caregivers require support to develop the technological understanding, capacity and skills necessary to assist children in relation to the digital environment. States parties should ensure that parents and caregivers have opportunities to gain digital literacy, to learn how technology can support the rights of children and to recognize a child who is a victim of online harm and respond appropriately. Special attention should be paid to the parents and caregivers of children in disadvantaged or vulnerable situations.

85. In supporting and guiding parents and caregivers regarding the digital environment, States parties should promote their awareness to respect children's growing autonomy and need for privacy, in accordance with their evolving capacities. States parties should take into account that children often embrace and experiment with digital opportunities and may encounter risks, including at a younger age than parents and caregivers may anticipate. Some children reported wanting more support and encouragement in their digital activities, especially where they perceived parents' and caregivers' approach to be punitive, overly restrictive or not adjusted to their evolving capacities.⁴⁰

86. States parties should take into account that support and guidance provided to parents and caregivers should be based on an understanding of the specificity and uniqueness of parent-child relations. Such guidance should support parents in sustaining an appropriate balance between the child's protection and emerging autonomy, based on mutual empathy and respect, over prohibition or control. To help parents and caregivers to maintain a balance between parental responsibilities and children's rights, the best interests of the child, applied

³⁹ General comment No. 24 (2019), para. 101; and CRC/C/156, para. 71.

⁴⁰ "Our rights in a digital world", p. 30.

together with consideration of the child's evolving capacities, should be the guiding principles. Guidance to parents and caregivers should encourage children's social, creative and learning activities in the digital environment and emphasize that the use of digital technologies should not replace direct, responsive interactions among children themselves or between children and parents or caregivers.

87. It is important that children separated from their families have access to digital technologies.⁴¹ Evidence has shown that digital technologies are beneficial in maintaining family relationships, for example, in cases of parental separation, when children are placed in alternative care, for the purposes of establishing relations between children and prospective adoptive or foster parents and in reuniting children in humanitarian crisis situations with their families. Therefore, in the context of separated families, States parties should support access to digital services for children and their parents, caregivers or other relevant persons, taking into consideration the safety and best interests of the child.

88. Measures taken to enhance digital inclusion should be balanced with the need to protect children in cases where parents or other family members or caregivers, whether physically present or distant, may place them at risk. States parties should consider that such risks may be enabled through the design and use of digital technologies, for example, by revealing the location of a child to a potential abuser. In recognition of those risks, They should require an approach integrating safety-by-design and privacy-by-design and ensure that parents and caregivers are fully aware of the risks and available strategies to support and protect children.

IX. Children with disabilities

89. The digital environment opens new avenues for children with disabilities to engage in social relationships with their peers, access information and participate in public decision-making processes. States parties should pursue those avenues and take steps to prevent the creation of new barriers and to remove existing barriers faced by children with disabilities in relation to the digital environment.

90. Children with different types of disabilities, including physical, intellectual, psychosocial, auditory and visual disabilities, face different barriers in accessing the digital environment, such as content in non-accessible formats, limited access to affordable assistive technologies at home, school and in the community and the prohibition of the use of digital devices in schools, health facilities and other environments. States parties should ensure that children with disabilities have access to content in accessible formats and remove policies that have a discriminatory impact on such children. They should ensure access to affordable assistive technologies, where needed, in particular for children with disabilities living in poverty, and provide awareness-raising campaigns, training and resources for children with disabilities, their families and staff in educational and other relevant settings so that they have sufficient knowledge and skills to use digital technologies effectively.

91. States parties should promote technological innovations that meet the requirements of children with different types of disabilities and ensure that digital products and services are designed for universal accessibility so that they can be used by all children without exception and without the need for adaptation. Children with disabilities should be involved in the design and delivery of policies, products and services that affect the realization of their rights in the digital environment.

92. Children with disabilities may be more exposed to risks, including cyberaggression and sexual exploitation and abuse, in the digital environment. States parties should identify and address the risks faced by children with disabilities, taking steps to ensure that the digital environment is safe for them, while countering the prejudice faced by children with disabilities that might lead to overprotection or exclusion. Safety information, protective strategies and public information, services and forums relating to the digital environment should be provided in accessible formats.

⁴¹ General comment No. 21 (2017), para. 35.

X. Health and welfare

93. Digital technologies can facilitate access to health services and information and improve diagnostic and treatment services for maternal, newborn, child and adolescent physical and mental health and nutrition. They also offer significant opportunities for reaching children in disadvantaged or vulnerable situations or in remote communities. In situations of public emergency or in health or humanitarian crises, access to health services and information through digital technologies may become the only option.

94. Children reported that they valued searching online for information and support relating to health and well-being, including on physical, mental and sexual and reproductive health, puberty, sexuality and conception.⁴² Adolescents especially wanted access to free, confidential, age-appropriate and non-discriminatory mental health and sexual and reproductive health services online.⁴³ States parties should ensure that children have safe, secure and confidential access to trustworthy health information and services, including psychological counselling services.⁴⁴ Those services should limit the processing of children's data to that which is necessary for the performance of the service and should be provided by professionals or those with appropriate training, with regulated oversight mechanisms in place. States parties should ensure that digital health products and services do not create or increase inequities in children's access to in-person health services.

95. States parties should encourage and invest in research and development that is focused on children's specific health needs and that promotes positive health outcomes for children through technological advances. Digital services should be used to supplement or improve the in-person provision of health services to children.⁴⁵ States parties should introduce or update regulation that requires providers of health technologies and services to embed children's rights within the functionality, content and distribution thereof.

96. States parties should regulate against known harms and proactively consider emerging research and evidence in the public health sector, to prevent the spread of misinformation and materials and services that may damage children's mental or physical health. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children's development and rights.⁴⁶

97. States parties should encourage the use of digital technologies to promote healthy lifestyles, including physical and social activity.⁴⁷ They should regulate targeted or age-inappropriate advertising, marketing and other relevant digital services to prevent children's exposure to the promotion of unhealthy products, including certain food and beverages, alcohol, drugs and tobacco and other nicotine products.⁴⁸ Such regulations relating to the digital environment should be compatible and keep pace with regulations in the offline environment.

98. Digital technologies offer multiple opportunities for children to improve their health and well-being, when balanced with their need for rest, exercise and direct interaction with their peers, families and communities. States parties should develop guidance for children, parents, caregivers and educators regarding the importance of a healthy balance of digital and non-digital activities and sufficient rest.

⁴² "Our rights in a digital world", p. 37.

⁴³ General comment No. 20 (2016), para. 59.

⁴⁴ *Ibid.*, paras. 47 and 59.

⁴⁵ *Ibid.*, paras. 47–48.

⁴⁶ General comment No. 15 (2013), para. 84.

⁴⁷ General comment No. 17 (2013), para. 13.

⁴⁸ General comment No. 15 (2013), para. 77.

XI. Education, leisure and cultural activities

A. Right to education

99. The digital environment can greatly enable and enhance children's access to high-quality inclusive education, including reliable resources for formal, non-formal, informal, peer-to-peer and self-directed learning. Use of digital technologies can also strengthen engagement between the teacher and student and between learners. Children highlighted the importance of digital technologies in improving their access to education and in supporting their learning and participation in extracurricular activities.⁴⁹

100. States parties should support educational and cultural institutions, such as archives, libraries and museums, in enabling access for children to diverse digital and interactive learning resources, including indigenous resources, and resources in the languages that children understand. Those and other valuable resources can support children's engagement with their own creative, civic and cultural practices and enable them to learn about those of others.⁵⁰ States parties should enhance children's opportunities for online and lifelong learning.

101. States parties should invest equitably in technological infrastructure in schools and other learning settings, ensuring the availability and affordability of a sufficient number of computers, high-quality and high-speed broadband and a stable source of electricity, teacher training on the use of digital educational technologies, accessibility and the timely maintenance of school technologies. They should also support the creation and dissemination of diverse digital educational resources of good quality in the languages that children understand and ensure that existing inequalities are not exacerbated, such as those experienced by girls. States parties should ensure that the use of digital technologies does not undermine in-person education and is justified for educational purposes.

102. For children who are not physically present in school or for those who live in remote areas or in disadvantaged or vulnerable situations, digital educational technologies can enable distance or mobile learning.⁵¹ States parties should ensure that there is proper infrastructure in place to enable access for all children to the basic utilities necessary for distance learning, including access to devices, electricity, connectivity, educational materials and professional support. They should also ensure that schools have sufficient resources to provide parents and caregivers with guidance on remote learning at home and that digital education products and services do not create or exacerbate inequities in children's access to in-person education services.

103. States parties should develop evidence-based policies, standards and guidelines for schools and other relevant bodies responsible for procuring and using educational technologies and materials to enhance the provision of valuable educational benefits. Standards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights, such as the use of digital technologies to document a child's activity and share it with parents or caregivers without the child's knowledge or consent.

104. States parties should ensure that digital literacy is taught in schools, as part of basic education curricula, from the preschool level and throughout all school years, and that such pedagogies are assessed on the basis of their results.⁵² Curricula should include the knowledge and skills to safely handle a wide range of digital tools and resources, including those relating to content, creation, collaboration, participation, socialization and civic

⁴⁹ "Our rights in a digital world", pp. 14, 16 and 30.

⁵⁰ General comment No. 17 (2013), para. 10.

⁵¹ Joint general recommendation No. 31 of the Committee on the Elimination of Discrimination against Women/general comment No. 18 of the Committee on the Rights of the Child (2019), para. 64; and Committee on the Rights of the Child, general comment No. 11 (2009), para. 61; and general comment No. 21 (2017), para. 55.

⁵² General comment No. 20 (2016), para. 47.

engagement. Curricula should also include critical understanding, guidance on how to find trusted sources of information and to identify misinformation and other forms of biased or false content, including on sexual and reproductive health issues, human rights, including the rights of the child in the digital environment, and available forms of support and remedy. They should promote awareness among children of the possible adverse consequences of exposure to risks relating to content, contact, conduct and contract, including cyberaggression, trafficking, sexual exploitation and abuse and other forms of violence, as well as coping strategies to reduce harm and strategies to protect their personal data and those of others and to build children's social and emotional skills and resilience.

105. It is of increasing importance that children gain an understanding of the digital environment, including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies. Teachers, in particular those who undertake digital literacy education and sexual and reproductive health education, should be trained on safeguards relating to the digital environment.

B. Right to culture, leisure and play

106. The digital environment promotes children's right to culture, leisure and play, which is essential for their well-being and development.⁵³ Children of all ages reported that they experienced pleasure, interest and relaxation through engaging with a wide range of digital products and services of their choice,⁵⁴ but that they were concerned that adults might not understand the importance of digital play and how it could be shared with friends.⁵⁵

107. Digital forms of culture, recreation and play should support and benefit children and reflect and promote children's differing identities, in particular their cultural identities, languages and heritage. They can facilitate children's social skills, learning, expression, creative activities, such as music and art, and sense of belonging and a shared culture.⁵⁶ Participation in cultural life online contributes to creativity, identity, social cohesiveness and cultural diversity. States parties should ensure that children have the opportunity to use their free time to experiment with information and communications technologies, express themselves and participate in cultural life online.

108. States parties should regulate and provide guidance for professionals, parents and caregivers and collaborate with digital service providers, as appropriate, to ensure that digital technologies and services intended for, accessed by or having an impact on children in their leisure time are designed, distributed and used in ways that enhance children's opportunities for culture, recreation and play. That can include encouraging innovation in digital play and related activities that support children's autonomy, personal development and enjoyment.

109. States parties should ensure that the promotion of opportunities for culture, leisure and play in the digital environment is balanced with the provision of attractive alternatives in the physical locations where children live. Especially in their early years, children acquire language, coordination, social skills and emotional intelligence largely through play that involves physical movement and direct face-to-face interaction with other people. For older children, play and recreation that involve physical activities, team sports and other outdoor recreational activities can provide health benefits, as well as functional and social skills.

110. Leisure time spent in the digital environment may expose children to risks of harm, for example, through opaque or misleading advertising or highly persuasive or gambling-like design features. By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child.

⁵³ General comment No. 17 (2013), para. 7.

⁵⁴ "Our rights in a digital world", p. 22.

⁵⁵ General comment No. 17 (2013), para. 33.

⁵⁶ *Ibid.*, para. 5.

111. Where States parties or businesses provide guidance, age ratings, labelling or certification regarding certain forms of digital play and recreation, they should be formulated so as not to curtail children's access to the digital environment as a whole or interfere with their opportunities for leisure or their other rights.

XII. Special protection measures

A. Protection from economic, sexual and other forms of exploitation

112. Children should be protected from all forms of exploitation prejudicial to any aspects of their welfare in relation to the digital environment. Exploitation may occur in many forms, such as economic exploitation, including child labour, sexual exploitation and abuse, the sale, trafficking and abduction of children and the recruitment of children to participate in criminal activities, including forms of cybercrime. By creating and sharing content, children may be economic actors in the digital environment, which may result in their exploitation.

113. States parties should review relevant laws and policies to ensure that children are protected against economic, sexual and other forms of exploitation and that their rights with regard to work in the digital environment and related opportunities for remuneration are protected.

114. States parties should ensure that appropriate enforcement mechanisms are in place and support children, parents and caregivers in gaining access to the protections that apply.⁵⁷ They should legislate to ensure that children are protected from harmful goods, such as weapons or drugs, or services, such as gambling. Robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements.

115. Considering States' obligations to investigate, prosecute and punish trafficking in persons, including its component actions and related conduct, States parties should develop and update anti-trafficking legislation so that it prohibits the technology-facilitated recruitment of children by criminal groups.

116. States parties should ensure that appropriate legislation is in place to protect children from the crimes that occur in the digital environment, including fraud and identity theft, and to allocate sufficient resources to ensure that crimes in the digital environment are investigated and prosecuted. States parties should also require a high standard of cybersecurity, privacy-by-design and safety-by-design in the digital services and products that children use, to minimize the risk of such crimes.

B. Administration of child justice

117. Children may be alleged to have, accused of or recognized as having infringed, cybercrime laws. States parties should ensure that policymakers consider the effects of such laws on children, focus on prevention and make every effort to create and use alternatives to a criminal justice response.

118. Self-generated sexual material by children that they possess and/or share with their consent and solely for their own private use should not be criminalized. Child-friendly channels should be created to allow children to safely seek advice and assistance where it relates to self-generated sexually explicit content.

119. States parties should ensure that digital technologies, surveillance mechanisms, such as facial recognition software, and risk profiling that are deployed in the prevention, investigation and prosecution of crimes are not used to unfairly target children suspected of

⁵⁷ General comment No. 16 (2013), para. 37.

or charged with criminal offences and are not used in a manner that violates their rights, in particular their rights to privacy, dignity and freedom of association.

120. The Committee recognizes that, where the digitization of court proceedings results in a lack of in-person contact with children, it may have a negative impact on rehabilitative and restorative justice measures built on developing relationships with the child. In such cases, and also where children are deprived of their liberty, States parties should provide in-person contact to facilitate children's ability to meaningfully engage with the courts and their rehabilitation.

C. Protection of children in armed conflict, migrant children and children in other vulnerable situations

121. The digital environment can provide children living in vulnerable situations, including children in armed conflict, internally displaced children, migrant, asylum-seeking and refugee children, unaccompanied children, children in street situations and children affected by natural disasters, with access to life-saving information that is vital for their protection. The digital environment can also enable them to maintain contact with their families, enable their access to education, health and other basic services and enable them to obtain food and safe shelter. States parties should ensure safe, secure, private and beneficial access for such children to the digital environment and protect them from all forms of violence, exploitation and abuse.

122. States parties should ensure that children are not recruited or used in conflicts, including armed conflicts, through the digital environment. That includes preventing, criminalizing and sanctioning the various forms of technology-facilitated solicitation and grooming of children, for example, though use of social networking platforms or chat services in online games.

XIII. International and regional cooperation

123. The cross-border and transnational nature of the digital environment necessitates strong international and regional cooperation, to ensure that all stakeholders, including States, businesses and other actors, effectively respect, protect and fulfil children's rights in relation to the digital environment. It is therefore vital that States parties cooperate bilaterally and multilaterally with national and international non-governmental organizations, United Nations agencies, businesses and organizations specialized in child protection and human rights in relation to the digital environment.

124. States parties should promote and contribute to the international and regional exchange of expertise and good practices and establish and promote capacity-building, resources, standards, regulations and protections across national borders that enable the realization of children's rights in the digital environment by all States. They should encourage the formulation of a common definition of what constitutes a crime in the digital environment, mutual legal assistance and the joint collection and sharing of evidence.

XIV. Dissemination

125. States parties should ensure that the present general comment is widely disseminated, including through use of digital technologies, to all relevant stakeholders, in particular parliaments and government authorities, including those responsible for cross-cutting and sectoral digital transformation, as well as members of the judiciary, business enterprises, the media, civil society and the public at large, educators and children, and is made available in multiple formats and languages, including age-appropriate versions.



Konvencija o pravima deteta

Distr.: Opšts
2. mart 2021.

Original: engleski

Komitet za prava deteta

Opšti komentar br. 25 (2021) o pravima deteta u vezi sa digitalnim okruženjem

I. Uvod

1. Deca koja su konsultovana za ovaj opšti komentar izjavila su da su digitalne tehnologije vitalne za njihov sadašnji život i budućnost: „Pomoću digitalne tehnologije možemo dobiti informacije iz celog sveta“; „[Digitalna tehnologija] me je upozнала sa glavnim aspektima toga kako sebe identifikujem“; „Kad ste tužni, internet vam može pomoći[da] vidite nešto što vam donosi radost“.¹
2. Digitalno okruženje se neprestano razvija i širi, obuhvatajući informacione i komunikacione tehnologije, uključujući digitalne mreže, sadržaj, usluge i aplikacije, povezane uređaje i okruženja, virtuelnu i proširenu stvarnost, veštačku inteligenciju, robotiku, automatizovane sisteme, algoritme i analitiku podataka, biometriju i tehnološkiuimplanta.²
3. Digitalno okruženje postaje sve važnije u većini aspekata života deteta, uključujući i u vremenima krize, jer se društvene funkcije, uključujući obrazovanje, vladine usluge i trgovinu, sve više oslanjaju na digitalne tehnologije. Ono pruža nove mogućnosti za ostvarivanje prava deteta, ali takođe predstavlja i rizik od njihovog kršenja ili zloupotrebe. Tokom konsultacija, deca su izrazila mišljenje da digitalno okruženje treba da podržava, promovise i štiti sigurnost i nepristrasnostnjihovogangažovanja: „Želeli bismo da nam vlada, tehnološke kompanije i nastavnici pomažu [u] upravljanju nepouzdanim informacijama na mreži.“; „Želela bih da razjasnim šta se zaista događa sa mojim podacima... Zašto ih prikupljati? Kako se prikupljaju?"; „Zabrinuta sam zbog deljenja mojih podataka“.³
4. Prava svakog deteta moraju se poštovati, štiti i ostvarivati u digitalnom okruženju. Inovacije u digitalnim tehnologijama utiču na život dece i njihova prava na načine koji su raznoliki i međusobno zavisni, čak i tamo gde deca sama ne pristupaju

¹“Ourrights in a digitalworld”, sumarni izveštaj o konsultovanju dece za ovaj opšti komentar, s. 14 i 22. Dostupno na <https://5rightsfoundation.com/uploads/Our%20Rights%20in%20a%20Digital%20World.pdf>. Sva pozivanja na stavove dece odnose se na ovaj izveštaj.

²Glosar terminologije dostupan je na web stranici Komiteta:

https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCRC%2fINF%2f9314&Lang=en

³“Ourrights in a digitalworld”, s 14, 16, 22 i 25.

internetu. Smislen pristup digitalnim tehnologijama može deci pomoći da ostvare čitav niz svojih građanskih, političkih, kulturnih, ekonomskih i socijalnih prava. Međutim, ako se ne dostigne digitalna inkluzija, postojeće nejednakosti će se verovatno povećati, a mogu se pojaviti i nove.

5. Ovaj opšti komentar temelji se na iskustvu Komiteta u pregledanju izveštaja država ugovornica, danu opšte rasprave o digitalnim medijima i pravima deteta, pravnoj praksi tela zaduženih za ljudska prava, preporukama Saveta za ljudska prava i posebnim procedurama Saveta, dve runde konsultacija sa državama, stručnjacima i drugim zainteresovanim stranama o konceptu i unapređenom nacrtu, kao i međunarodnim konsultacijama sa 709 deteta koja žive u najrazličitijim okolnostima u 28 zemalja, u nekoliko regiona.

6. Ovaj opšti komentar treba čitati zajedno sa drugim relevantnim opštim komentarima Komiteta i njegovim smernicama u vezi sa sprovođenjem Opcionog protokola uz Konvenciju o prodaji dece, dečjoj prostituciji i dečjoj pornografiji.

II. Cilj

7. U ovom opštem komentaru, Komitet objašnjava kako Države ugovornice treba da primene Konvenciju u odnosu na digitalno okruženje i daje smernice o relevantnim zakonodavnim, političkim i drugim merama, kako bi obezbedile potpuno poštovanje svojih obaveza prema Konvenciji i opcionim protokolima uz nju u smislunogućnosti, rizika i izazova u promovisanju, poštovanju, zaštiti i ostvarivanju svih prava deteta u digitalnom okruženju.

III. Opšti principi

8. Sledeća četiri principa pružaju okvir u kome treba posmatrati sprovođenje svih ostalih prava iz Konvencije. Oni bi trebalo da posluže kao vodilja za određivanje mera potrebnih za garantovanje ostvarivanja prava deteta u odnosu na digitalno okruženje.

A. Nediskriminacija

9. Pravo na nediskriminaciju zahteva da države članice osiguraju da sva deca imaju jednak i efikasan pristup digitalnom okruženju na smisaone načine.⁴ Države ugovornice treba da preduzmu sve mere neophodne za prevazilaženje digitalne isključenosti. To obuhvata pružanje besplatnog i bezbednog pristupa deci na namenskim javnim lokacijama i ulaganje u politike i programe koji podržavaju pristup svakom detetu i osmišljenu upotrebu digitalnih tehnologija u obrazovnim okruženjima, zajednicama i domovima.

10. Deca mogu biti diskriminisana isključivanjem iz upotrebe digitalnih tehnologija i usluga ili izlaganjem komunikacijama ispunjenim mržnjom ili nepravednim tretmanom upotrebom tih tehnologija. Drugi oblici diskriminacije mogu nastati kada se automatizovani procesi koji rezultiraju filtriranjem informacija, profilisanjem ili donošenjem odluka zasnivaju na pristrasnim, delimičnim ili neetično pribavljenim podacima o detetu.

11. Komitet poziva države ugovornice da preduzmu proaktivne mere za sprečavanje diskriminacije na osnovu pola, invaliditeta, socijalno-ekonomskog stanja, etničkog ili nacionalnog porekla, jezika ili bilo kom drugom osnovu, kao i diskriminacije dece koja

⁴Opšti komentar br. 9 (2006), para. 37–38.

pripadaju manjinama ili autohtonim narodima, dece tražilaca azila, izbeglica i migranata, lezbejki, homoseksualaca, biseksualne, transrodne i interseksulne dece, dece koja su žrtve i su preživeli trgovinu ljudima ili seksualnu eksploataciju, dece u alternativnoj nezi, dece lišene slobode i dece u drugim ranjivim situacijama. Potrebne su i posebne mere za otklanjanje digitalnog podvajanja rodnojosnovi kada su u pitanju devojčice, kao i za osiguravanje da se posebna pažnja posveti pristupu, digitalnoj pismenosti, privatnosti i bezbednosti na mreži.

B. Najbolji interesi deteta

12. Najbolji interes deteta je dinamičan koncept koji zahteva procenu koja odgovara konkretnom kontekstu.⁵ Digitalno okruženje prvobitno nije bilo dizajnirano za decu, ali igra značajnu ulogu u dečjim životima. Države ugovornice treba da osiguraju da je u svim akcijama u vezi sa obezbeđivanjem, uređivanjem, dizajniranjem, upravljanjem i upotrebom digitalnog okruženja najbolji interes svakog deteta primarna briga.

13. Države ugovornice treba da uključe nacionalna i lokalna tela koja nadgledaju ispunjavanje prava dece u takve aktivnosti. Razmatrajući najbolje interese deteta, trebalo bi da uzmu u obzir sva dečja prava, uključujući njihova prava da traže, primaju i prenose informacije, da budu zaštićena od povređivanja, kao i da njihovi stavovi dobiju odgovarajuću težinu, odnosno da obezbede transparentnost u proceni najboljih interesa deteta i kriterijuma koji su primenjeni.

C. Pravo na život, opstanak i razvoj

14. Mogućnosti koje pruža digitalno okruženje igraju sve presudniju ulogu u razvoju dece i mogu biti od vitalnog značaja za život i opstanak dece, posebno u kriznim situacijama. Države ugovornice treba da preduzmu sve odgovarajuće mere da zaštite decu od rizika po njihovo pravo na život, opstanak i razvoj. Rizici koji se odnose na sadržaj, kontakt, ponašanje i dogovore uključuju, između ostalog, nasilni i seksualni sadržaj, sajber-napad i uznemiravanje, kockanje, eksploataciju i zloupotrebu, uključujući seksualno eksploataciju i zloupotrebu, kao i promovisanje ili podsticanje na samoubistvo ili aktivnosti opasne po život, uključujući kriminalce ili naoružane grupe označene kao terorističke ili nasilno ekstremističke. Države ugovornice treba da identifikuju i reše nove rizike sa kojima se deca suočavaju u različitim kontekstima, između ostalog i tako što će saslušati njihove stavove o prirodi određenih rizika sa kojima se suočavaju.

15. Upotreba digitalnih uređaja ne bi smela biti štetna, niti sme biti zamena za lične interakcije između dece ili između dece i roditelja ili staralaca. Države ugovornice treba da obrate posebnu pažnju na efekte tehnologije u najranijim godinama života, kada je plastičnost mozga maksimalna, a socijalno okruženje, posebno odnosi sa roditeljima i staraocima, presudni za oblikovanje kognitivnog, emocionalnog i socijalnog razvoja dece. U ranim godinama mogu biti potrebne mere predostrožnosti, u zavisnosti od dizajna, namene i upotrebe tehnologija. Obuku i savete o pravilnoj upotrebi digitalnih uređaja treba pružiti roditeljima, staraocima, vaspitačima i drugim relevantnim akterima, uzimajući u obzir istraživanja o efektima digitalnih tehnologija na razvoj dece, posebno tokom kritičnih neuroloških brzih promena tokom⁶ ranog detinjstva i adolescencije.

⁵Opšti komentar br. 14 (2013), para. 1.

⁶Opšti komentar br. 24 (2019), para. 22; iOpšti komentar br. 20 (2016), para. 9–11.

D. Poštovanje stavova deteta

16. Deca su izjavila da im digitalno okruženje pruža ključne mogućnosti da se njihovi glasovi čuju u pitanjima koje ih se tiču.⁷ Upotreba digitalnih tehnologija može pomoći u ostvarivanju učešća dece na lokalnom, nacionalnom i međunarodnom nivou.⁸ Države ugovornice treba da promovišu svest o digitalnim sredstvima i odgovarajućipristup kako bi deca mogla da izraze svoje stavove, kao i da ponude obuku i podršku deci da učestvuju ravnopravno sa odraslima, po potrebianonimno, tako da mogu biti efikasni zagovornici njihovih prava, pojedinačno i kao grupa.

17. Kada razvijaju zakonodavstvo, politike, programe, usluge i obuku o pravima deteta u vezi sa digitalnim okruženjem, Države ugovornice treba da uključe svu decu, saslušaju njihove potrebe i daju odgovarajuću težinu njihovim stavovima. One bi trebalo da osiguraju da pružaoci digitalnih usluga aktivno stupaju u interakciju sa decom, primenjujućiodgovarajuće mere zaštite, i da njihove stavove uzmu u obzir prilikom razvoja proizvoda i usluga.

18. Države ugovornice se podstiču da koriste digitalno okruženje za konsultacije sa decom o relevantnim zakonodavnim, administrativnim i drugim merama i da obezbede da se njihovi stavovi ozbiljno razmotre i da učešće dece ne rezultira neprimerenim nadgledanjem ili prikupljanjem podataka koji krše njihovo pravo na privatnost, slobodu misli i stavova. One bi trebalo da osiguraju da konsultativni procesi obuhvate decu koja nemaju pristup tehnologiji ili veštine da je koriste.

IV. Razvojni kapaciteti

19. Države ugovornice treba da poštuju evolutivne sposobnosti deteta kao principa koji omogućavaprocen njihovog postepenog sticanja kompetencija, razumevanja i delovanja.⁹ Taj proces je posebno značajan u digitalnom okruženju, gde se deca mogu više angažovati nezavisno od nadzora roditelja i staraoca. Rizici i mogućnosti povezani sa dečijim angažovanjem u digitalnom okruženju menjaju se u zavisnosti od njihove starosti i stepena razvoja. Države ugovornice bi trebalo da se rukovode tim zaključcima kad god osmišljavaju mere za zaštitu dece u digitalnom okruženju ili im olakšavaju pristup. Dizajn mera prilagođenih uzrastu treba da de zasniva na najboljim i najsavremenijim dostupnim istraživanjima iz različitih disciplina.

20. Države ugovornice treba da uzmu u obzir promenljivi položaj dece i njihovog delovanja u savremenom svetu, kompetenciju i razumevanje dece, koja nejednako razvijaju svoje veštine i aktivnosti, kao i raznoliku prirodu rizika. Ta razmatranja moraju biti u ravnoteži sa značajem ostvarivanja njihovih prava u podržanim okruženjima i opsegom pojedinačnih iskustava i okolnosti.¹⁰ Države ugovornice treba da osiguraju da pružaoci digitalnih usluga nude usluge koje odgovaraju kapacitetima dece, koji se razvijaju.

21. U skladu sa dužnošću država da pružaju odgovarajućupomoć roditeljima i staraocima u izvršavanju njihovih obaveza u odgajanju dece, države ugovornice treba da podižu svest roditelja i starlaca o potrebi poštovanja dečje autonomije, kapaciteta i privatnosti, koje se razvijaju. One bi trebalo da podrže roditelje i staraoce u sticanju digitalne pismenosti, kao i svesti o rizicima po decu, kako bi im omogućili da pomognu

⁷Ourrights in a digitalworld”, s. 17.

⁸Opšti komentar br. 14 (2013), para. 89–91.

⁹Opšti komentar br. 7 (2005), para. 17; i Opšti komentar br. 20 (2016), para. 18 i 20.

¹⁰Opšti komentar br. 20 (2016), para. 20.

deci u ostvarivanju njihovih pravau vezi sa digitalnim okruženjem, uključujući pravo na zaštitu.

V. Opšte mere primene Država ugovornica

22. Prilike za ostvarivanje prava deteta i njihovu zaštitu u digitalnom okruženju zahtevaju širok spektar zakonodavnih, administrativnih i drugih mera, uključujući mere predostrožnosti.

A. Zakonodavstvo

23. Države ugovornice trebalo bi da pregledaju, usvoje i ažuriraju nacionalno zakonodavstvo u skladu sa međunarodnim standardima o ljudskim pravima, kako bi se osiguralo da je digitalno okruženje kompatibilno sa pravima utvrđenim u Konvenciji i njenim opcionim protokolima. Zakonodavstvo treba da ostane relevantno u kontekstu tehnološkog napretka i novih praksi. Države ugovornice bi trebalo da uvedu obavezu upotrebe procene uticaja na prava deteta radi ugrađivanja ovih prava u zakonodavstvo, budžetska izdvajanja i druge administrativne odluke koje se odnose na digitalno okruženje, kao i da promovišu njihovu upotrebu među javnim telima i preduzećima koja se odnose na digitalno okruženje.¹¹

B. Sveobuhvatna politika i strategija

24. Države ugovornice treba da osiguraju da se nacionalne politike koje se odnose na prava deteta posebno bave digitalnim okruženjem i da shodno tome primenjuju propise, industrijske kodekse, standarde dizajna i akcione planove, što sve treba redovno ocenjivati i ažurirati. Takve nacionalne politike treba da imaju za cilj pružanje deci mogućnosti da imaju koristi od angažovanja u digitalnom okruženju i obezbeđivanje njihovog sigurnog pristupa ovom okruženju.

25. Zaštita dece na mreži treba da bude integrisana u nacionalne politike zaštite dece. Države ugovornice treba da primene mere koje štite decu od rizika, uključujući sajber-napade, kao i seksualno iskorišćavanje i zloupotrebe dece pomoću digitalne tehnologije i namreži, da obezbede istragu takvih zločina, kao i obeštećenje i podršku deci koja su žrtve. Takođe bi trebalo da se pozabave potrebama dece u nepovoljnim ili ranjivim situacijama, uključujući pružanje informacija prilagođenih deci koje se, kada je to potrebno, prevode na relevantne jezike manjina.

26. Države ugovornice treba da obezbede funkcionisanje efikasnih mehanizama zaštite dece na mreži, kao i politike zaštite, istovremeno poštujući i druga prava deteta, u svim sredinama u kojima deca imaju pristup digitalnom okruženju, koje uključuje dom, obrazovne ustanove, sajber-kafe, omladinske centre, biblioteke, kao i zdravstvene ustanove i okruženja alternativne nege.

C. Koordinacija

27. Da bi obuhvatile unakrsne posledice digitalnog okruženja po dečja prava, države ugovornice treba da identifikuju vladino telo koje je zaduženo da koordinira politike, smernice i programe koji se odnose na prava deteta, između centralnih vladinih odeljenja

¹¹Opšti komentar br.5 (2003), para. 45; Opšti komentar br. 14 (2013), para. 99; i Opšti komentar br. 16 (2013), para. 78–81

i različitih nivoa vlasti.¹² Takav nacionalni mehanizam za koordinaciju treba da se poveže sa školama i sektorom informacionih i komunikacionih tehnologija i da saraduje sa preduzećima, civilnim društvom, akademskom zajednicom i organizacijama, radi ostvarivanja dečjih prava u odnosu na digitalno okruženje na među-sektorskom, nacionalnom, regionalnom i lokalnom nivou.¹³ Prema potrebi, trebalo bi da se oslanja na tehnološku i drugu relevantnu ekspertizu unutar i izvan vlade i da bude nezavisno ocenjivanokada je u pitanju njegova efikasnostu ispunjavanju njegovih obaveza.

D. Alokacija resursa

28. Države ugovornice treba da mobilišu, alociraju i koriste javne resurse za sprovođenje zakonodavstva, politika i programa za potpuno ostvarivanje prava deteta u digitalnom okruženju, za poboljšanje digitalne inkluzije koja je potrebna za rešavanje sve većeg uticaja digitalnog okruženja na život dece, kao i za promociju ravnopravnosti pristupa, odnosno pristupačnosti usluga i povezivanja.¹⁴

29. Tamo gde resursi doprinose iz poslovnog sektora ili se dobijaju putem međunarodne saradnje, države ugovornice treba da obezbede da treće strane ne ometaju i ne utiču negativnoma njihov vlastiti mandat, mobilizaciju prihoda, budžetska izdvajanja i rashode.¹⁵

E. Prikupljanje podataka i istraživanje

30. Redovno ažurirani podaci i istraživanja su presudni za razumevanje implikacija digitalnog okruženja za život dece, procenu njegovog uticaja na njihova prava i procenu efikasnosti državnih intervencija. Države ugovornice trebalo bi da osiguraju prikupljanje čvrstih, sveobuhvatnih podataka, pomoću adekvatnih resursa, koji su razvrstani prema starosti, polu, invaliditetu, geografskom položaju, etničkom i nacionalnom poreklu i socijalno-ekonomskom stanju. Takvi podaci i istraživanja, uključujući istraživanja koja uključuju decu i sprovode ih deca, treba da posluže kao osnovaza zakonodavstvo, politiku i praksu i treba da budu dostupni u javnom domenu.¹⁶ Prikupljanje podataka i istraživanje u vezi sa digitalnim životom dece mora poštovati njihovu privatnost i ispunjavati najviše etičke standarde.

F. Nezavisninadzor

31. Države ugovornice treba da osiguraju da mandati nacionalnih institucija za ljudska prava i drugih odgovarajućih nezavisnih institucija pokrivaju prava deteta u digitalnom okruženju i da su u mogućnosti da primaju, istražuju i postupaju po žalbama dece i njihovih predstavnika.¹⁷ Tamo gde postoje nezavisna nadzorna tela koja nadgledaju aktivnosti u vezi sa digitalnim okruženjem, nacionalne institucije za ljudska prava treba da blisko saraduju sa takvim telima na efikasnom izvršavanju svog mandata u pogledu dečjih prava.

¹²Opšti komentar br.5 (2003), para. 37.

¹³Isto, para. 27 i 39.

¹⁴Opšti komentar br. 19 (2016), para. 21.

¹⁵Isto, para. 27 (b).

¹⁶Opšti komentar br. 5 (2003), para. 48 i 50.

¹⁷Opšti komentar br. 2 (2002), para. 2 i 7.

G. Širenje informacija, podizanje svesti i obuka

32. Države ugovornice trebalo bi da šire informacije i vode kampanje za podizanje svesti o pravima deteta u digitalnom okruženju, posebno se fokusirajući na one čije akcije imaju direktan ili indirektan uticaj na decu. Trebalo bi da obezbede obrazovne programe za decu, roditelje i staraoce, širu javnost i kreatore politika, kako bi oni unapredili svoje znanje o dečijim pravima u vezi sa mogućnostima i rizicima povezanim sa digitalnim proizvodima i uslugama. Takvi programi treba da uključuju informacije o tome kako deca mogu imati koristi od digitalnih proizvoda i usluga i razviti svoju digitalnu pismenost i veštine, kako zaštititi dečju privatnost i sprečiti viktimizaciju, kao i kako prepoznati dete koje je žrtva povređivanja počinjenog na mreži ili van nje, i na odgovarajući način reagovali. Takvi programi treba da budu se zasnivaju na istraživanjima i konsultacijama sa decom, roditeljima i staraocima.

33. Profesionalci koji rade za sa decom i poslovnim sektorom, odnosno sa njima, uključujući tehnološku industriju, trebalo bi da prođu obuku koja uključuje kako digitalno okruženje utiče na prava deteta u različitim kontekstima, načine na koje deca ostvaruju svoja prava u digitalnom okruženju i kako pristupaju i koriste tehnologije. Takođe bi trebalo da prođu obuku o primeni međunarodnih standarda ljudskih prava na digitalno okruženje. Države ugovornice treba da osiguraju da se profesionalcima koji rade na svim nivoima obrazovanja, pre i tokom službe, obezbedi obuka koja se odnosi na digitalno okruženje, kako bi se podržao razvoj njihovog znanja, veština i prakse.

H. Saradnja sa civilnim društvom

34. Države ugovornice treba u razvoj, primenu, praćenje i ocenu zakona, politika, planova i programa koji se odnose na prava detetasisematski da uključuju civilno društvo, što obuhvatai grupe koje vode deca, kao i nevladine organizacije koje rade na polju dečijih prava i one koji se bave digitalnim okruženjem. Takođe bi trebalo da osiguraju da organizacije civilnog društva mogu da sprovedu svoje aktivnosti koje se odnose na promociju i zaštitu dečjih prava u odnosu na digitalno okruženje.¹⁸

I. Prava deteta i poslovni sektor

35. Poslovni sektor, uključujući neprofitne organizacije, direktno i indirektno utiče na prava deteta u pružanju usluga i proizvoda koji se odnose na digitalno okruženje. Preduzeća treba da poštuju prava deteta i spreče i isprave zloupotrebu njihovih prava u vezi sa digitalnim okruženjem. Države ugovornice imaju obavezu da osiguraju da preduzeća ispunjavaju te obaveze.¹⁹

36. Države ugovornice treba da preduzmu mere, uključujući kroz razvoj, praćenje, primenu i ocenu zakona, propisa i politika, kako bi osigurale da preduzeća poštuju svoje obaveze da spreče da se njihove mreže ili mrežne usluge koriste na načine koji uzrokuju ili doprinose kršenjima ili zloupotrebi dečjih prava, uključujući njihova prava na privatnost i zaštitu, kao i da obezbede deci, roditeljima i staraocima brzo i efikasno obeštećenje. Takođe bi trebalo da podstaknu preduzeća da pružaju javne informacije i dostupne i pravovremene savete za podršku bezbednim i korisnim digitalnim aktivnostima dece.

37. Države ugovornice su dužne da zaštite decu od kršenja njihovih prava od strane poslovnih preduzeća, uključujući pravo na zaštitu od svih oblika nasilja u digitalnom

¹⁸Isto, para. 7.

¹⁹Opšti komentar br. 16 (2013), para. 28, 42 i 82.

okruženju. Iako preduzeća možda nisu direktno umešana u vršenje štetnih dela, ona mogu prouzrokovati ili doprineti kršenju prava dece na slobodu od nasilja, uključujući kroz dizajn i pružanje digitalnih usluga. Države ugovornice treba da uspostave, nadgledaju i sprovede zakone i propise usmerene na sprečavanje kršenja prava na zaštitu od nasilja, kao i one čiji je cilj istraga, presuđivanje i ispravljanje kršenja prava u slučaju da se ona pojave u odnosu na digitalno okruženje.²⁰

38. Države ugovornice treba da zahtevaju od poslovnog sektora da preduzme detaljnu analizu prava deteta, posebno da izvrši procenu uticaja na prava deteta i obelodani ih javnosti, s posebnim osvrtom na raznorodne i, povremeno, ozbiljne uticaje digitalnog okruženja na decu.²¹ One treba da preduzmu odgovarajuće korake da spreče, nadgledaju, istražuju i kañnjavaju kršenja prava deteta od strane preduzeća.

39. Pored razvijanja zakonodavstva i politika, države ugovornice trebalo bi da zahtevaju od svih preduzeća koja utiču na prava deteta u vezi sa digitalnim okruženjem da primene regulatorne okvire, industrijske kodekse i uslove usluga koji poštuju najviše standarde etičnosti, privatnosti i bezbednosti vezano za dizajn, inženjering, razvoj, rad, distribuciju i marketing njihovih proizvoda i usluga. To uključuje preduzeća koja za ciljnu grupu ili kao krajnje korisnike imaju decu, ili na drugi način utiču na decu. Od takvih preduzeća treba da zahtevaju da se pridržavaju visokih standarda transparentnosti i odgovornosti i podstiču ih da preduzimaju mere za inovacije u najboljem interesu deteta. Onetaođe treba da zahtevaju da preduzeća pružaju objašnjenja o uslovima pružanja svojih uslugadeći, koja suprilagođenih njihovom starosnom dobu, odnosno roditeljima i staraocima vrlo male dece.

J. Komercijalno oglašavanje i marketing

40. Digitalno okruženje obuhvata preduzeća koja se finansijski oslanjaju na obradu ličnih podataka radi ciljnih sadržaja koji donose prihod ili koji se plaćaju, a takvi procesi namerno i nenamerno utiču na digitalna iskustva dece. Mnogi od tih procesa uključuju veći broj komercijalnih partnera, čime se stvara lanac komercijalnih aktivnosti i obrade ličnih podataka koji mogu dovesti do kršenja ili zloupotrebe dečjih prava, što uključuje karakteristike dizajna oglašavanja koje navode aktivnost detetaka ekstremnijim sadržajima, automatizovana obaveštenja koja mogu prekinuti spavanje ili upotrebu ličnih podataka detetala njegove lokacije u cilju potencijalno štetnih komercijalnih sadržaja.

41. Države ugovornice treba da imaju na umu najbolje interese deteta pri regulisanju oglašavanja i marketinga namenjenog deci i dostupnog deci. Sponzorstvo, plasman proizvoda i svi drugi oblici komercijalno vođenog sadržaja treba jasno razlikovati od svih ostalih sadržaja i oni ne bi trebalo da ponavljaju rodne ili rasne stereotipe.

42. Države ugovornice trebalo bi zakonom da zabraneprofilisanje ili ciljanje dece bilo kog uzrasta u komercijalne svrhe na osnovu digitalnog zapisa njihovih stvarnih ili izvedenih karakteristika, uključujući grupne ili kolektivne podatke, ciljanje po osnovu povezivanja ili afiniteta. Praksama koje se oslanjaju na neuromarketing, emocionalnu analitiku, dubinsko oglašavanje i oglašavanje u okruženjima virtuelne i proširene stvarnosti za promociju proizvoda, aplikacija i usluga takođe treba zabraniti direktno ili indirektno angažovanje sa decom.

²⁰Isto, para. 60.

²¹Isto, para. 50 i 62-65.

K. Pristup pravdi i obeštećenju

43. Deca se iz različitih razloga suočavaju sa posebnim izazovima u pristupu pravdi koji se odnose na digitalno okruženje. Takvi izazovi, između ostalog, nastaju zbog nedostatka zakona kojim se sankcionišu kršenja prava deteta posebno u vezi sa digitalnim okruženjem, poteškoća u pribavljanju dokaza ili identifikovanju počilaca ili zato što deca i njihovi roditelji ili staraoci nemaju znanja o svojim pravima ili o onome što predstavlja kršenje ili zloupotreba njihovih prava u digitalnom okruženju. Dodatni izazovi mogu se pojaviti ako se od dece zahteva da otkriju osetljive ili privatne aktivnosti na mreži ili zbog straha od odmazde vršnjaka ili socijalne isključenosti.

44. Države ugovornice treba da osiguraju da su odgovarajući i efikasni pravni i van-pravni pravni mehanizmi za kršenje dečjih prava koji se odnose na digitalno okruženje široko poznati i lako dostupni svoj deci i njihovim predstavnicima. Mehanizmi za žalbe i prijavljivanje treba da budu besplatni, sigurni, poverljivi, odzivni, prilagođeni deci i raspoloživi u lako dostupnim formatima. Države ugovornice takođe treba da obezbede mogućnost kolektivne žalbe, uključujući kolektivne tužbe i parnice od javnog interesa, kao i pravnu ili drugu odgovarajuću pomoć, uključujući specijalizovane usluge, za decu čija su prava povređena u digitalnom okruženju ili putem njega.

45. Države ugovornice treba da uspostave, koordinišu i redovno nadgledaju i procenjuju okvire za prijavljivanje takvih slučajeva i pružanje efikasne podrške deci koja su žrtve.²²Ovi okviri bi trebalo da uključuju mere za identifikaciju, terapiju i naknadnostaranje i socijalnu reintegraciju dece koja su žrtve. Obuka o identifikaciji dece koja su žrtve treba da bude uključena u mehanizme prijavljivanja, uključujući i pružaoce digitalnih usluga. Mere u takvom okviru treba da budu višestlane i prilagođene deci, kako bi se sprečila reviktimizacija i sekundarna viktimizacija deteta u kontekstu istražnih i sudskih procesa. To može zahtevati specijalizovanu zaštitu poverljivosti i ispravljanje štete povezane sa digitalnim okruženjem.

46. Odgovarajuća odšteta uključuje povraćaj, obeštećenje i pružanje satisfakcije i može zahtevati izvinjenje, ispravku, uklanjanje nezakonitog sadržaja, pristup uslugama psihološkog oporavka ili druge mere.²³ U vezi sa kršenjima u digitalnom okruženju, korektivni mehanizmi treba da uzmu u obzir ranjivost dece i potrebu da budu brzi da bi zaustavili tekuću i buduću štetu. Države ugovornice treba da garantuju da ne dolazi do ponavljanja prestupa, uključujući i reformu relevantnih zakona i politika i njihovu efikasnu primenu.

47. Digitalne tehnologije unose dodatnu složenost u istrage i krivično gonjenje zločina protiv dece, koji mogu prelaziti državne granice. Države ugovornice treba da se pozabave načinima na koje upotreba digitalnih tehnologija može olakšati ili ometati istragu i krivično gonjenje zločina protiv dece i preduzeti sve raspoložive preventivne mere, mere izvršenja i obeštećenja, što uključuje saradnju sa međunarodnim partnerima. One treba da pruže specijalizovanu obuku za službenike koji sprovode zakone, tužioce i sudije u vezi sa kršenjem prava deteta posebno povezanim sa digitalnim okruženjem, što uključuje i međunarodnu saradnju.

48. Deca se mogu suočiti sa posebnim poteškoćama u dobijanju obeštećenja kada su preduzeća zloupotrebila njihova prava u digitalnom okruženju, posebno u kontekstu svog globalnog poslovanja.²⁴ Države ugovornice trebalo bi da razmotre mere za poštovanje, zaštitu i ispunjavanje dečjih prava u kontekstu eksteritorijalnih aktivnosti i operacija preduzeća, pod uslovom da postoji razumna veza između države i dotičnog ponašanja.

²²Opšti komentar br. 21 (2017), para. 22. Videti i rezoluciju 60/147 Generalne skupštine, aneks.

²³Opšti komentar br. 5 (2003), para. 24.

²⁴Opšti komentar br. 16 (2013), para. 66–67.

One treba da obezbede da preduzeća pružaju efikasne mehanizme za podnošenje žalbi; takvi mehanizmi, međutim, ne bi trebalo da sprečavaju decu da pristupe državnim obeštećenjima. Takođe bi trebalo da osiguraju da agencije sa nadzornim ovlašćenjima relevantnim za prava deteta, poput onih koje se odnose na zdravlje i bezbednost, zaštitu podataka i prava potrošača, obrazovanje i oglašavanje i marketing, istražuju žalbe i pružaju odgovarajućekorektivne mere za kršenje ili zloupotrebu prava deteta u digitalnom okruženju.²⁵

49. Države ugovornice treba da pruže deci informacije prilagođene deci i njihovom uzrastu, jezikom prilagođenim deci, o njihovim pravima i o mehanizmima za prijavljivanje i žalbe, kao i o uslugama i korektivnim merama koje su im na raspolaganju u slučajevima kada su njihova prava u vezi sa digitalnim okruženjem povređena ili zloupotrebljena. Takve informacije takođe treba pružiti roditeljima, staraocima i profesionalcima koji rade sa i za decu.

VI. Građanska prava i slobode

A. Pristup informacijama

50. Digitalno okruženje pruža jedinstvenu priliku deci da ostvare pravo na pristup informacijama. U tom pogledu, informacioni i komunikacioni mediji, uključujući digitalni i mrežni sadržaj, obavljaju važnu funkciju.²⁶ Države ugovornice treba da obezbede da deca imaju pristup informacijama u digitalnom okruženju i da je uživanje tog prava ograničeno samo kada je to predviđeno zakonom i neophodno u svrhe predviđene članom 13 Konvencije.

51. Države ugovornice treba da obezbede i podrže proizvodnju digitalnog sadržaja za decu koji odgovara njihovom uzrastu i koji ih osnažuje, au skladu sa razvojnim kapacitetima dece, kao i da obezbede deci pristup raznorodnim informacijama, uključujući informacije koje poseduju javne ustanove, o kulturi, sportu, umetnosti, zdravlju, građanskim i političkim pitanjima i pravima deteta.

52. Države ugovornice treba da podstiču proizvodnju i širenje takvog sadržaja u različitim formatima i iz više nacionalnih i međunarodnih izvora, uključujući novinske medije, emitere, muzeje, biblioteke i obrazovne, naučne i kulturne organizacije. One bi posebno trebalo da nastoje da poboljšaju pružanje raznolikog, pristupačnog i korisnog sadržaja za decu sa invaliditetom i decu koja pripadaju etničkim, jezičkim, autohtonim i drugim manjinskim grupama. Sposobnost pristupa relevantnim informacijama na jezicima koje deca razumeju može imati značajan pozitivan uticaj na ravnopravnost.²⁷

53. Države ugovornice treba da osiguraju da su sva deca informisana o raznolikim i kvalitetnim informacijama na mreži da ih mogu lako pronaći, uključujući sadržaje nezavisne od komercijalnih ili političkih interesa. Trebalo bi da obezbede da automatizovano pretraživanje i filtriranje informacija, uključujući sisteme preporuka, ne daju prioritet plaćenim sadržajima sa komercijalnom ili političkom motivacijom nad dečijim izborima ili po cenu prava deteta na informacije.

54. Digitalno okruženje može uključivati rodno stereotipne, diskriminatorne, rasističke, nasilne, pornografske i eksploatacione informacije, kao i lažne narative, dezinformacije, kao i informacije koje podstiču decu da se bave nezakonitim ili štetnim aktivnostima. Takve informacije mogu poticati iz više izvora, uključujući druge

²⁵Isto, para. 30 i 43.

²⁶Opšti komentar br. 7 (2005), para. 35; iOpšti komentar br. 20 (2016), para. 47.

²⁷Opšti komentar br. 17 (2013), para. 46; iOpšti komentar br. 20 (2016), para. 47–48.

korisnike, kreatora komercijalnog sadržaja, seksualne prestupnike ili oružane grupe označene kao terorističke ili nasilno ekstremističke. Države ugovornice treba da zaštite decu od štetnog i nepouzdanog sadržaja i obezbede da relevantna preduzeća i drugi dobavljači digitalnog sadržaja razviju i primene smernice kojima će deci omogućiti bezbedan pristup raznovrsnim sadržajima, priznajući prava deteta na informacije i slobodu izražavanja, istovremeno ih štiteći od takvih štetnih materijala u skladu sa njihovim pravima i razvojnim kapacitetima.²⁸ Sva ograničenja u radu bilo kog internet, elektronskog ili drugog sistema za širenje informacija treba da budu u skladu sa članom 13 Konvencije.²⁹ Države ugovornice ne bi trebalo da namerno ometaju ili omogućavaju drugim akterima da ometaju snabdevanje električnom energijom, mobilne mreže ili internet veze u bilo kom geografskom području, bilo delimično ili u celini, što može imati za posledicu ometanje pristupa dece informacijama i komunikaciji.

55. Države ugovornice treba da podstaknu pružaoce digitalnih usluga koje deca koriste da primenjuju koncizno i razumljivo obeležavanje sadržaja, na primer o primerenosti za određeni uzrast ili verodostojnosti sadržaja. Takođe bi trebalo da podstiču obezbeđivanje dostupnih smernica, obuka, obrazovnih materijala i mehanizama izveštavanja, za decu, roditelje i staraoce, vaspitače i relevantne profesionalne grupe.³⁰ Sistemi dizajnirani prema uzrastu ili sadržaju tako da zaštite decu od sadržaja neprikladnog uzrastu treba da budu u skladu sa principom minimiziranja podataka.

56. Države ugovornice treba da osiguraju da se pružaoce digitalnih usluga pridržavaju relevantnih smernica, standarda i kodeksa³¹ i sprovode zakonita, neophodna i proporcionalna pravila moderiranja sadržaja. Kontrole sadržaja, školski sistemi za filtriranje i druge tehnologije orijentisane na bezbednost ne bi trebalo da se koriste za ograničavanje pristupa dece informacijama u digitalnom okruženju; treba ih koristiti samo za sprečavanje priliva materijala štetnog za decu. Moderiranje sadržaja i kontrole sadržaja treba da budu uravnoteženi sa pravom na zaštitu od kršenja drugih prava dece, posebno njihovih prava na slobodu izražavanja i privatnost.

57. Profesionalni kodeksi ponašanja koje postavljaju novinski mediji i druge relevantne organizacije treba da sadrže smernice o tome kako prijaviti digitalne rizike i mogućnostikoje se odnose na decu. Takva uputstva treba da rezultiraju izveštavanjem zasnovanim na dokazima koji ne otkrivaju identitet dece koja su žrtve i koja su preživela, odnosno izveštavanjem u skladu sa međunarodnim standardima ljudskih prava.

B. Sloboda izražavanja

58. Pravo dece na slobodu izražavanja uključuje slobodu traženja, primanja i prenošenja informacija i ideja svih vrsta, korišćenjem bilo kog medija po njihovom izboru. Deca su izjavila³² da im digitalno okruženje nudi značajan prostor za izražavanje njihovih ideja, mišljenja i političkih stavova. Za decu u nepovoljnim ili ranjivim situacijama, tehnološki olakšana interakcija sa drugima koji dele njihova iskustva može im pomoći da se izraze.

59. Sva ograničenja prava deteta na slobodu izražavanja u digitalnom okruženju, poput filtera, uključujući mere bezbednosti, trebalo bi da budu zakonita, neophodna i proporcionalna. Obrazloženje takvih ograničenja trebalo bi da bude transparentno i da se deci saopštava na jeziku prilagođenom uzrastu. Države ugovornice treba da pruže deci

²⁸Opšti komentar br. 16 (2013), para. 58; iOpšti komentar br. 7 (2005), para. 35.

²⁹Komitet za ljudska prava, Opšti komentar br. 34 (2011), para. 43.

³⁰Opšti komentar br. 16 (2013), para. 19 i 59.

³¹Isto, para. 58 i 61.

³²“Ourrights in a digitalworld”, s. 16.

informacije i mogućnosti za obuku o tome kako efikasno ostvariti to pravo, posebno kako bezbedno kreirati i deliti digitalni sadržaj, uz poštovanje prava i dostojanstva drugih i ne kršeći zakone, poput zakona koji se odnosi na podsticanje mržnje i nasilja.

60. Kada deca izražavaju svoje političke ili druge stavove i identitete u digitalnom okruženju, mogu privući kritiku, neprijateljstvo, pretnje ili kaznu. Države ugovornice treba da zaštite decu od sajber agresije i pretnji, cenzure, nelegalnog pribavljanja podataka i digitalnog nadzora. Decu ne bi trebalo krivično goniti zbog izražavanja mišljenja u digitalnom okruženju, osim ako ne krše ograničenja predviđena krivičnim zakonodavstvom koja su kompatibilna sa članom 13 Konvencije.

61. S obzirom na postojanje komercijalnih i političkih motiva za promociju određenih pogleda na svet, države ugovornice treba da osiguraju da upotrebe automatizovanih procesa filtriranja informacija, profilisanja, marketinga i donošenja odluka ne zamenjuju, ne manipulišu ili ne ometaju sposobnost dece da formiraju i izraze svoje mišljenje u digitalnom okruženju.

C. Sloboda misli, savesti i veroispovesti

62. Države ugovornice treba da poštuju pravo deteta na slobodu misli, savesti i veroispovesti u digitalnom okruženju. Komitet podstiče države ugovornice da uvedu ili ažuriraju propise o zaštiti podataka i standarde dizajna koji identifikuju, definišu i zabranjuju prakse kojima se manipuliše ili ometa pravo dece na slobodu misli i verovanja u digitalnom okruženju, na primer emocionalnom analitikom ili zaključivanjem. Automatizovani sistemi mogu da se koriste za zaključivanje o unutrašnjem stanju deteta. Treba osigurati da se automatizovani sistemi ili sistemi za filtriranje informacija ne koriste da bi uticali na dečje ponašanje ili emocije ili ograničili njihove mogućnosti ili razvoj.

63. Države ugovornice trebalo bi da osiguraju da deca ne budu kažnjavana zbog svoje religije ili uverenja ili da im se budućemogućnosti na bilo koji drugi način ograničavaju. Ostvarivanje prava deteta na ispoljavanje svoje religije ili uverenja u digitalnom okruženju može biti podložno samo ograničenjima koja su zakonita, neophodna i proporcionalna.

D. Sloboda udruživanja i mirnog okupljanja

64. Digitalno okruženje može deci omogućiti da formiraju svoj socijalni, verski, kulturni, etnički, seksualni i politički identitet i da učestvuju u povezanim zajednicama i na javnim prostorima za raspravu, kulturnu razmenu, socijalnu koheziju i različitost.³³ Deca su izjavila da im digitalno okruženje pruža dragocene mogućnosti da se sretnu, ostvare razmenu i raspravljaju sa vršnjacima, donosiocima odluka i drugima koji dele njihova interesovanja.³⁴

65. Države ugovornice treba da osiguraju da njihovi zakoni, propisi i politike štite pravo dece da učestvuju u organizacijama koje deluju delimično ili isključivo u digitalnom okruženju. Deca ne mogu imati ograničenja u ostvarivanju svog prava na slobodu udruživanja i mirnog okupljanja u digitalnom okruženju, osim ograničenja koja su zakonita, neophodna i proporcionalna.³⁵ Takvo učešće samo po sebi ne bi trebalo da rezultira negativnim posledicama po tu decu, kao što su isključenje iz škole, ograničenje

³³Opšti komentar br. 17 (2013), para. 21; iOpšti komentar br. 20 (2016), para. 44–45.

³⁴“Ourrights in a digitalworld”, s. 20.

³⁵Komitet za ljudska prava, Opšti komentar br. 37 (2020), para. 6 i 34.

ili lišavanje budućih mogućnosti ili stvaranje policijskog profila. Takvo učešće treba da bude sigurno, privatno i bez nadzora javnih ili privatnih subjekata.

66. Javna vidljivost i mogućnosti umrežavanja u digitalnom okruženju takođe mogu podržati aktivizam koji vode deca i mogu osnažiti decu kao zagovornike ljudskih prava. Komitet prepoznaje da digitalno okruženje omogućava deci, uključujući decu zaštitnike ljudskih prava, kao i decu u osetljivim situacijama, da međusobno komuniciraju, zagovaraju svoja prava i osnivaju udruženja. Države ugovornice treba da ih podrže, što uključuje omogućavanje stvaranja određenih digitalnih prostora, i da im osiguraju sigurnost.

E. Pravo na privatnost

67. Privatnost je od vitalnog značaja za aktivnosti dece, njihovo dostojanstvo i sigurnost, kao i za ostvarivanje njihovih prava. Lični podaci dece obrađuju se kako bi im se pružile obrazovne, zdravstvene i druge pogodnosti. Pretnje privatnosti dece mogu nastati prikupljanjem i obradom podataka od strane javnih institucija, preduzeća i drugih organizacija, kao i od kriminalnih aktivnosti kao što je krađa identiteta. Pretnje mogu nastati i zbog sopstvenih aktivnosti dece i aktivnosti članova porodice, vršnjaka ili drugih, na primer, ako roditelji dele fotografije na mreži ili stranac deli informacije o detetu.

68. Podaci mogu, između ostalog, sadržati informacije o dečjem identitetu, aktivnostima, lokaciji, komunikaciji, emocijama, zdravlju i vezama. Određene kombinacije ličnih podataka, uključujući biometrijske podatke, mogu jedinstveno identifikovati dete. Digitalne prakse, kao što su automatizovana obrada podataka, profilisanje, ciljanje ponašanja, obavezna verifikacija identiteta, filtriranje informacija i masovni nadzor postaju rutina. Takva praksa može dovesti do proizvoljnog ili nezakonitog mešanja u pravo dece na privatnost; mogu imati štetne posledice na decu, što može da utiče na njih u kasnijim fazama njihovog života.

69. Ometanje privatnosti deteta dozvoljeno je samo ako nije ni proizvoljno ni nezakonito. Svako takvo uplitanje stoga treba da bude predviđeno zakonom, s ciljem da služi legitimnoj svrsi, pridržava se principa minimizacije podataka, i mora biti srazmerno i dizajnirano da poštuje najbolji interes deteta, a ne sme biti u suprotnosti sa odredbama ili ciljevima Konvencije.

70. Države ugovornice treba da preduzmu zakonodavne, administrativne i druge mere kako bi osigurale da privatnost dece poštuju i štite sve organizacije i u svim sredinama koje obrađuju njihove podatke. Zakonodavstvo treba da uključuje jake zaštitne mere, transparentnost, nezavisan nadzor i pristup korektivnim merama. Države ugovornice treba da zahtevaju integrisanje dizajna privatnosti u digitalne proizvode i usluge koji utiču na decu. One treba redovno da preispituju zakone o privatnosti i zaštiti podataka i osiguraju da postupci i prakse sprečavaju namerno ili slučajno kršenje privatnosti dece. Tamo gde se šifrovanje smatra odgovarajućim sredstvom, države ugovornice treba da razmotre odgovarajuće mere koje omogućavaju otkrivanje i prijavljivanje seksualnog iskorišćavanja i zloupotrebe dece ili materijala za seksualnu zloupotrebu dece. Takve mere moraju biti strogo ograničene u skladu sa principima zakonitosti, neophodnosti i proporcionalnosti.

71. Kada se traži saglasnost za obradu podataka o detetu, države ugovornice treba da obezbede da dete saglasnost daje slobodno i na osnovu raspoloživih informacija, ili, u zavisnosti od starosti deteta i njegovih razvojnih mogućnosti, to učini roditelj ili staralac, i da sesaglasnost dobije pre obrade tih podataka. Kada se smatra da je saglasnost deteta nedovoljna, te da je za obradu ličnih podataka deteta potrebna saglasnost roditelja, države potpisnice treba da zahtevaju da organizacije koje obrađuju takve podatke potvrde da je

saglasnost data na osnovu raspoloživih informacija, da je smislena, i da je daje detetov roditelj ili staralac.

72. Države ugovornice treba da obezbede da deca i njihovi roditelji ili staraoci mogu lako pristupiti uskladištenim podacima, ispraviti podatke koji su netačni ili zastareli i izbrisati podatke koje nezakonito ili nepotrebno čuvaju javni organi, privatna lica ili druga tela, shodno razumnim i zakonitim ograničenjima.³⁶ Dalje bi trebalo da obezbede pravo dece da povuku svoj pristanak i usprotive se obradi ličnih podataka tamo gde onaj ko kontroliše podatke ne pokaže legitimne, preovlađujuće razloge za obradu. One takođe treba da pruže informacije deci, roditeljima i staraocima o takvim pitanjima, na jeziku prilagođenom deci i u pristupačnim formatima.

73. Lični podaci dece trebalo bi da budu dostupni samo državnim vlastima, organizacijama i pojedincima, koji su zakonom određeni da ih obrađuju, u skladu sa odgovarajućim procesnim garancijama kao što su redovne revizije i mere odgovornosti.³⁷ Podaci deteta prikupljeni u definisane svrhe, u bilo kom okruženju, uključujući digitalizovane kriminalne evidencije, treba da budu zaštićeni i korišćeni isključivo u te svrhe i ne smeju se nezakonito ili nepotrebno čuvati ili koristiti u druge svrhe. Tamo gde se informacije dostupne u jednom okruženju, a mogu legitimno koristiti detetu u drugom okruženju, na primer, u kontekstu školovanja i tercijarnog obrazovanja, upotreba takvih podataka treba da bude transparentna, odgovorna i, prema potrebi, podložna pristanku deteta, roditelja ili staraoca.

74. Zakoni i mere o privatnosti i zaštiti podataka ne bi trebalo da proizvoljno ograničavaju druga prava dece, poput njihovog prava na slobodu izražavanja ili zaštitu. Države ugovornice treba da osiguraju da zakonodavstvo o zaštiti podataka poštuje dečju privatnost i lične podatke u vezi sa digitalnim okruženjem. Stalnim tehnološkim inovacijama, opseg digitalnog okruženja se proširuje i uključuje još više usluga i proizvoda, poput odeće i igračaka. Kako okruženja u kojima deca provode vreme postaju „povezana“, upotrebom ugrađenih senzora povezanih na automatizovane sisteme, države ugovornice treba da obezbede da proizvodi i usluge koji doprinose takvim okruženjima podležu snažnoj zaštiti podataka i drugim propisima i standardima o privatnosti. To uključuje javna okruženja, poput ulica, škola, biblioteka, sportskih i zabavnih objekata i poslovnih prostora, uključujući prodavnice i bioskope, i dom.

75. Bilo koji digitalni nadzor dece, zajedno sa bilo kojom povezanom automatizovanom obradom ličnih podataka, treba da poštuje pravo detetana privatnost i ne sme se sprovesti rutinski, neselektivno ili bez znanja detetali, u slučaju vrlo male dece, njihovog roditelja ili staraoca; niti bi se to trebalo odvijati bez prava na prigovor takvom nadzoru, u komercijalnim okruženjima i obrazovnim ustanovama i ustanovama za zaštitu, i uvek bi trebalo razmotriti sredstva koja najmanje narušavaju privatnost raspoloživa da bi se ispunila željena svrha.

76. Digitalno okruženje predstavlja posebne probleme roditeljima i staraocima u poštovanju prava dece na privatnost. Tehnologije koje nadgledaju aktivnosti na mreži iz bezbednosnih razloga, poput uređaja i servisaza praćenje, ako se ne primene pažljivo, mogu sprečiti dete da pristupi liniji za pomoć ili da pretražuje osetljive informacije. Države ugovornice trebalo bi da savetuju decu, roditelje i staraoce, kao i javnost o važnosti prava deteta na privatnost i o tome kako njihova sopstvena praksa može to pravo da ugrozi. Takođe bi ih trebalo savetovati o praksama kroz koje mogu poštovati i zaštititi privatnost dece u odnosu na digitalno okruženje, istovremeno ih štiteći. Nadzor roditelja i staralaca nad digitalnom aktivnošću deteta treba da bude proporcionalan i u skladu sa detetovim kapacitetima koji se razvijaju.

³⁶Komitet za ljudska prava, Opšti komentar br. 16 (1988), para. 10.

³⁷Isto; takođe, Komitet za prava deteta, Opšti komentar br. 20 (2016), para. 46.

77. Mnoga deca koriste mrežne avatare ili pseudonime koji štite njihov identitet, a takve prakse mogu biti važne u zaštiti privatnosti dece. Države ugovornice trebalo bi da zahtevaju pristup koji integriše bezbednost-po-dizajnu i privatnost-po-dizajnu anonimnosti, istovremeno osiguravajući da se anonimne prakse rutinski ne koriste za sakrivanje štetnog ili nezakonitog ponašanja, poput sajber agresije, govora mržnje ili seksualnog iskorišćavanja i zloupotrebe. Zaštita detetove privatnosti u digitalnom okruženju može biti od vitalnog značaja u okolnostima kada roditelji ili starijaci sami predstavljaju pretnju za bezbednost deteta ili kada su u sukobu oko staranja o detetu. Takvi slučajevi mogu zahtevati dalju intervenciju, kao i porodično savetovanje ili druge usluge, kako bi se zaštitilo detetovo pravo na privatnost.

78. Pružaoci preventivnih ili savetodavnih usluga za decu u digitalnom okruženju treba da budu izuzeti od bilo kakvih zahteva da dete dobije roditeljski pristanak kako bi pristupilo takvim uslugama.³⁸ Takve usluge treba pružati prema visokim standardima privatnosti i zaštite dece.

F. Registrovanje rođenja i pravo na identitet

79. Države ugovornice treba da promovisu upotrebu sistema digitalne identifikacije koji omogućavaju registrovanje i službeno priznavanje rođenja sve novorođene dece od strane nacionalnih vlasti, kako bi se olakšao pristup uslugama, uključujući zdravstvo, obrazovanje i dobrobit. Odsustvo registrovanja rođenja olakšava kršenje prava deteta koje ono ima po Konvenciji i njenim opcionim protokolima. Države ugovornice trebalo bi da koriste najsavremeniju tehnologiju, uključujući mobilne jedinice za registraciju, kako bi osigurale pristup registrovanju rođenja, posebno za decu u udaljenim oblastima, izbegličku i migrantsku decu, decu u riziku i decu u marginalizovanim situacijama, kao i decu rođenu pre uvođenje sistema digitalne identifikacije. Da bi takvi sistemi koristili deci, države ugovornice bi trebalo da sprovedu kampanje za podizanje svesti, uspostave mehanizme praćenja, promovisu angažovanje zajednice i obezbede efikasnu koordinaciju između različitih aktera, uključujući službenike za civilni status, sudije, beležnike, zdravstvene službe i osoblje agencija za zaštitu dece. Takođe bi trebalo da osiguraju postojanje snažnog okvira za zaštitu privatnosti i podataka.

VII. Nasilje nad decom

80. Digitalno okruženje može otvoriti nove mogućnosti za vršenje nasilja nad decom, olakšavajući stvaranje situacija u kojima deca doživljavaju nasilje i/ili mogu potpasti pod uticaj da nanese štetu sebi ili drugima. Krize, poput pandemije, mogu dovesti do povećanog rizika od povređivanja na mreži, s obzirom na to da deca u tim okolnostima provode više vremena na virtuelnim platformama.

81. Seksualni prestupnici mogu da koriste digitalne tehnologije za podsticanje dece u seksualne svrhe i za učešće u seksualnoj zloupotrebi dece na mreži, na primer, direktnim prenosom video zapisa, produkcijom i distribucijom materijala sa seksualnom zloupotrebom dece i seksualnim iznuđivanjem. Oblici digitalno olakšanog nasilja i seksualnog iskorišćavanja i zloupotrebe takođe se mogu pojaviti u krugu poverenja deteta, porodice ili prijatelja ili, za adolescente, od strane intimnih partnera, a mogu uključivati i sajber-agresiju, uključujući maltretiranje i pretnje ugledu, kreiranje ili deljenje seksualizovanog teksta ili slika bez konsenzusa, kao što je sopstvenogenerisan sadržaj na onsovu podsticanja i/ili prinude, i promocija samopovređujućih ponašanja, poput sečenja, samoubilačkog ponašanja ili poremećaja u ishrani. Tamo gde su deca vršila

³⁸Opšti komentar br. 20 (2016), para. 60.

takve radnje, države ugovornice treba da slede preventivne, zaštitne i korektivne pravne pristupe prema uključenoj deci kad god je to moguće.³⁹

82. Države ugovornice treba da preduzmu zakonodavne i administrativne mere za zaštitu dece od nasilja u digitalnom okruženju, uključujući redovnu reviziju, ažuriranje i provođenje snažnih zakonodavnih, regulatornih i institucionalnih okvira koji štite decu od prepoznatih i novih rizika od svih oblika nasilja u digitalnom okruženju. Takvi rizici uključuju fizičko ili mentalno nasilje, povredu ili zloupotrebu, zanemarivanje ili maltretiranje, eksploataciju i zloupotrebu, uključujući seksualno iskorišćavanje i zloupotrebu, trgovinu decom, rodno zasnovano nasilje, sajber-agresiju, sajber-napade i informacijski rat. Države ugovornice treba da primene mere sigurnosti i zaštite u skladu sa razvojnim kapacitetima deteta.

83. Digitalno okruženje može otvoriti nove načine za neredovne grupe, uključujući oružane grupe označene kao terorističke ili nasilno ekstremističke, da vrbuju i iskorišćavaju decu da bi se uključila u nasilje ili učestvovala u njemu. Države ugovornice trebalo bi da osiguraju da zakonodavstvo zabranjuje vrbovanje dece od strane terorističkih ili nasilno ekstremističkih grupa. Decu optuženu za krivična dela u tom kontekstu trebalo bi tretirati prvenstveno kao žrtve, ali ako se optužuju, trebalo bi primeniti sistem pravosuđa za decu.

VIII. Porodično okruženje i alternativno staranje

84. Mnogi roditelji i staraoci zahtevaju podršku da bi razvili tehnološko razumevanje, kapacitet i veštine neophodne za pomoć deci u odnosu na digitalno okruženje. Države ugovornice treba da osiguraju da roditelji i staraoci imaju mogućnosti da steknu digitalnu pismenost, da nauče kako tehnologija može podržati prava dece i kako da prepoznaju dete koje je žrtva povređivanja na mreži, kao i kako da reaguju na odgovarajući način. Posebnu pažnju treba posvetiti roditeljima i staraocima dece u nepovoljnim ili ranjivim situacijama.

85. Podržavajući i usmeravajući roditelje i staraoce u vezi sa digitalnim okruženjem, države ugovornice treba da unaprede njihovu svest da poštuju rastuću autonomiju dece i potrebu za privatnošću, u skladu sa njihovim razvojnim kapacitetima. Države ugovornice treba da uzmu u obzir da deca često prihvataju digitalne mogućnosti i sa njima eksperimentišu, i da se mogu suočiti sa rizicima, uključujući i mlađem dobu od onog koje roditelji i staraoci mogu da predvide. Neka deca su izjavila da žele veću podršku i ohrabrenje u svojim digitalnim aktivnostima, posebno tamo gde su smatrala da je pristup roditelja i staraoca kazneni, preterano restriktivan ili neprilagođen njihovim razvojnim kapacitetima.⁴⁰

86. Države ugovornice treba da uzmu u obzir da podrška i smernice koje se pružaju roditeljima i staraocima treba da se zasnivaju na razumevanju specifičnosti i jedinstvenom odnosu roditelja i deteta. Takve smernice treba da podrže roditelje u održavanju odgovarajuće ravnoteže između zaštite deteta i njegove rastuće autonomije, zasnovane na uzajamnoj empatiji i poštovanju, umesto zabrane ili kontrole. Da bi se roditeljima i staraocima pomoglo da održe ravnotežu između roditeljskih odgovornosti i prava deteta, vodeći principi treba da budu najbolji interesi deteta, primenjeni zajedno sa uzimanjem u obzir razvojnih kapaciteta deteta. Smernice za roditelje i staraoce treba da podstiču dečje društvene, kreativne i obrazovne aktivnosti u digitalnom okruženju i naglašavaju da

³⁹Opšti komentar br. 24 (2019), para. 101; takođe CRC/C/156, para. 71.

⁴⁰“Ourrights in a digital world”, s. 30.

upotreba digitalnih tehnologija ne bi trebalo da zameni direktne reaktivne interakcije između same dece ili između dece i roditelja ili staratelja.

87. Važno je da deca odvojena od porodice imaju pristup digitalnim tehnologijama.⁴¹ Dokazi svedoče da su digitalne tehnologije korisne u održavanju porodičnih odnosa, na primer, u slučajevima roditeljske razdvojenosti, kada su deca smeštena u alternativnostarateljstvo, radi uspostavljanja odnosa između dece i budućihusvojitelja ili hranitelja i ponovnog spajanja dece sa njihovim porodicama u humanitarnim kriznim situacijama. Stoga, u kontekstu razdvojenih porodica, države ugovornice treba da podrže pristup digitalnim uslugama za decu i njihove roditelje, staraoci ili druge relevantne osobe, uzimajući u obzir bezbednost i najbolje interese deteta.

88. Preduzete mere za poboljšanje digitalne inkluzije treba da budu uravnotežene sa potrebom zaštite dece u slučajevima kada ih roditelji ili drugi članovi porodice ili staraoci, bilo fizički prisutni ili udaljeni, mogu dovesti u rizik. Države ugovornice treba da uzmu u obzir da se takvi rizici mogu olakšati dizajnom i upotrebom digitalnih tehnologija, na primer otkrivanjem lokacije deteta potencijalnom zlostavljaču. One trebalo da zahtevaju pristup koji integriše bezbednost-po-dizajnu i privatnost-po-dizajnu i da osiguraju da roditelji i staraoci budu potpuno svesni rizika i dostupnih strategija za podršku i zaštitu dece.

IX. Deca sa invaliditetom

89. Digitalno okruženje otvara nove mogućnosti deci sa invaliditetom da se uključe u društvene odnose sa vršnjacima, pristupe informacijama i učestvuju u javnim procesima donošenja odluka. Države ugovornice treba da slede te pravce i preduzmu korake da spreče stvaranje novih prepreka i uklone postojeće prepreke sa kojima se suočavaju deca sa invaliditetom u odnosu na digitalno okruženje.

90. Deca sa različitim vrstama invaliditeta, uključujući fizičke, intelektualne, psihosocijalne, slušne i vizuelne smetnje, suočavaju se sa različitim preprekama u pristupu digitalnom okruženju, poput sadržaja u nepristupačnim formatima, ograničenog pristupa asistivnim tehnologijama u kući, u školi i u zajednici, i sprečavanja upotrebe digitalnih uređaja u školama, zdravstvenim ustanovama i drugim sredinama. Države ugovornice treba da obezbede da deca sa invaliditetom imaju pristup sadržajima u pristupačnim formatima i uklone politike koje imaju diskriminatorski uticaj na takvu decu. One bi trebalo da obezbede pristup asistivnim tehnologijama, gde je to potrebno, posebno za decu sa invaliditetom koja žive u siromaštvu, i da obezbede kampanje za podizanje svesti, obuku i resurse za decu sa invaliditetom, njihove porodice i osoblje u obrazovnim i drugim relevantnim uslovima, tako da oni mogu steknu dovoljno znanja i veština za efikasnu upotrebu digitalnih tehnologija.

91. Države ugovornice treba da promovišu tehnološke inovacije koje ispunjavaju zahteve dece sa različitim vrstama invaliditeta i osiguraju da su digitalni proizvodi i usluge dizajnirani za univerzalnu dostupnost, tako da ih mogu koristiti sva deca bez izuzetka i bez potrebe za prilagođavanjem. Deca sa invaliditetom treba da budu uključena u dizajniranje i realizaciju politika, proizvoda i usluga koji utiču na ostvarivanje njihovih prava u digitalnom okruženju.

92. Deca sa invaliditetom mogu biti izložena rizicima, uključujući sajber-agresiju i seksualno iskorišćavanje i zloupotrebu, u digitalnom okruženju. Države ugovornice treba da identifikuju i reše rizike sa kojima se suočavaju deca sa invaliditetom, preduzimajući

⁴¹Opšti komentar br. 21 (2017), para. 35.

mere da osiguraju da digitalno okruženje za tu decu bude bezbedno, istovremeno se borećiprotiv predrasuda sa kojima se suočavaju deca sa invaliditetom,a koje mogu dovesti do preterane zaštite ili isključenja. Informacije o bezbednosti, zaštitne strategije i javne informacije, usluge i forumi koji se odnose na digitalno okruženje treba da se obezbede u pristupačnim formatima.

X. Zdravlje i blagostanje

93. Digitalne tehnologije mogu olakšati pristup zdravstvenim uslugama i informacijama i poboljšati usluge dijagnostike i lečenja kada su u pitanju fizičko i mentalno zdravlje i ishrana majki, novorođenčadi, dece i adolescenata. One takođe nude značajne mogućnostida se dopre do dece u nepovoljnim ili ranjivim situacijama ili u udaljenim zajednicama. U vanrednim situacijama ili u zdravstvenim ili humanitarnim krizama pristup zdravstvenim uslugama i informacijama putem digitalnih tehnologija može postati jedina opcija.

94. Deca su izjavila da cene traženje informacija i podrške u vezi sa zdravljem i blagostanjem putem interneta, što uključuje pitanja fizičkog, mentalnog i seksualnog i reproduktivnog zdravlja, puberteta, seksualnosti i začeća.⁴² Adolescenti su posebno želeli pristup besplatnim, poverljivim, uzrastu prikladnim i nediskriminatorskim uslugama mentalnog zdravlja, kao i uslugama seksualnog i reproduktivnog zdravlja na mreži.⁴³ Države ugovornice treba da osiguraju da deca imaju bezbedan, siguran i poverljiv pristup pouzdanim zdravstvenim informacijama i uslugama, uključujući usluge psihološkog savetovanja.⁴⁴Te usluge treba da ograniče obradu dečijih podataka na onu koja je neophodna za obavljanje usluge i treba da je pružaju profesionalci ili oni koji imaju odgovarajuću obuku, uz uspostavljanje regulisanih mehanizama nadzora. Države ugovornice treba da osiguraju da digitalni zdravstveni proizvodi i usluge ne stvaraju ili povećavaju nejednakost u pristupu dece zdravstvenim uslugama.

95. Države ugovornice treba da podstiču i ulažu u istraživanje i razvoj koji su usredsređeni na posebne zdravstvene potrebe dece i koji promovišu pozitivne zdravstvene ishode za decu kroz tehnološki napredak. Digitalne usluge treba koristiti za dopunu ili poboljšanje pružanja zdravstvenih usluga deci.⁴⁵ Države ugovornice treba da uvedu ili ažuriraju propise kojima se od dobavljača zdravstvenih tehnologija i usluga zahteva da u njihovu funkcionalnost, sadržaj i distribucijuugrade prava deteta.

96. Države ugovornice treba da uvedu regulativu protiv poznatih uzroka štete i da proaktivno razmotre nova istraživanja i dokaze u javnom zdravstvenom sektoru, kako bi sprečile širenje dezinformacija i materijala i usluga koji mogu naštetiti mentalnom ili fizičkom zdravlju dece. Moguće je da budu potrebne i mere za sprečavanje nezdravog bavljenja digitalnim igrama ili društvenim medijima, kao što je uvođenje regulative protiv digitalnog dizajna koji podriva razvoj i prava deteta.⁴⁶

97. Države ugovornice treba da podstiču upotrebu digitalnih tehnologija za promociju zdravih stilova života, uključujući fizičku i društvenu aktivnost.⁴⁷ Trebalo bi da regulišu ciljano ili uzrastu neprikladno oglašavanje, marketing i druge relevantne digitalne usluge kako bi sprečile izloženost dece promociji nezdravih proizvoda, uključujući određenu

⁴²“Ourrights in a digitalworld”, s. 37.

⁴³Opšti komentar br. 20 (2016), para. 59.

⁴⁴Isto, para. 47 i 59.

⁴⁵Isto, para 47-48.

⁴⁶Opšti komentar br. 15 (2013), para. 84.

⁴⁷Opšti komentar br. 17 (2013), para. 13.

hranu i pića, alkohol, drogu i duvan i druge nikotinske proizvode.⁴⁸ Takvi propisi koji se odnose na digitalno okruženje treba da budu kompatibilni i da idu ukorak sa propisima u vanmrežnom okruženju.

98. Digitalne tehnologije nude deci višestruke mogućnosti da poboljšaju svoje zdravlje i blagostanje, kada se uravnoteže sa njihovom potrebom za odmorom, vežbanjem i direktnom interakcijom sa vršnjacima, porodicama i zajednicama. Države ugovornice trebalo bi da razviju smernice za decu, roditelje, staraoce i vaspitače u vezi sa značajem zdrave ravnoteže između digitalnih i nedigitalnih aktivnosti i dovoljnog odmora.

XI. Obrazovanje, rasonoda i kulturne aktivnosti

A. Pravo na obrazovanje

99. Digitalno okruženje može u velikoj meri omogućiti i poboljšati pristup dece visokokvalitetnom inkluzivnom obrazovanju, uključujući pouzdane resurse za formalno, neformalno, neformalno, vršnjačko i samostalno učenje. Korišćenje digitalnih tehnologija takođe može ojačati angažman između učenika, kao između nastavnika i učenika. Deca su istakla značaj digitalnih tehnologija u poboljšanju njihovog pristupa obrazovanju i u podršci njihovom učenju i učešću u vannastavnim aktivnostima.⁴⁹

100. Države ugovornice trebalo bi da podrže obrazovne i kulturne institucije, poput arhiva, biblioteka i muzeja, u omogućavanju deci pristupa različitim digitalnim i interaktivnim resursima za učenje, uključujući autohtone resurse, kao i resurse na jezicima koje deca razumeju. Ti, kao i drugi vredni resursi, mogu da podrže dečju angažovanost u sopstvenim kreativnim, građanskim i kulturnim praksama i omoguće im da uče o drugima.⁵⁰ Države ugovornice treba da poboljšaju mogućnosti dece za onlajn i celoživotno učenje.

101. Države ugovornice treba da ulože ravnopravno u tehnološku infrastrukturu u školama i u druge nastavne okvire, osiguravajući dostupnost i pristupačnost dovoljnog broja računara, visokokvalitetne i brze širokopolasne mreže i stabilan izvor električne energije, obuku nastavnika za korišćenje digitalnih obrazovnih tehnologija, pristupačnost i pravovremeno održavanje školskih tehnologija. Takođe bi trebalo da podrže stvaranje i širenje različitih digitalnih obrazovnih resursa dobrog kvaliteta na jezicima koje deca razumeju i obezbede da postojeće nejednakosti ne budu pogoršane, poput onih koje doživljavaju devojčice. Države ugovornice treba da osiguraju da upotreba digitalnih tehnologija ne podriva neposredno obrazovanje i da je opravdana u obrazovne svrhe.

102. Za decu koja nisu fizički prisutna u školi ili za ona koja žive u udaljenim oblastima ili u nepovoljnim ili ranjivim situacijama, digitalne obrazovne tehnologije mogu omogućiti učenje na daljinu ili mobilno učenje.⁵¹ Države ugovornice treba da osiguraju postojanje odgovarajuće infrastrukture koja omogućava svoj deci pristup osnovnim uslužnim programima neophodnim za učenje na daljinu, uključujući pristup uređajima, električnoj energiji, povezivanju, obrazovnim materijalima i profesionalnoj podršci. Takođe bi trebalo da obezbede da škole imaju dovoljno resursa da roditeljima i staraocima pruže smernice o učenju na daljinu kod kuće, kao i da proizvodi i usluge digitalnog

⁴⁸Opšti komentar br. 15 (2013), para. 77.

⁴⁹“Ourrights in a digitalworld”, s. 14, 16 i 30.

⁵⁰Opšti komentar br. 17 (2013), para. 10.

⁵¹Zajednička opšta preporuka br. 31 Komiteta za ukidanje diskriminacije prema ženama/Opšti komentar br. 18 Komiteta za prava deteta (2019), para. 64; takođe Komitet za prava deteta, Opšti komentar br. 11 (2009), para. 61; kao i Opšti komentar br. 21 (2017), para. 55.

obrazovanja ne stvaraju ili pogoršavaju nejednakosti u pristupu dece obrazovnim uslugama.

103. Države ugovornice trebalo bi da razviju politike, standarde i smernice, zasnovane na raspoloživoj evidenciji, za škole i druga relevantna tela odgovorna za nabavku i upotrebu obrazovnih tehnologija i materijala, kako bi poboljšale obezbeđivanje dragocene obrazovne koristi. Standardi za digitalne obrazovne tehnologije treba da osiguraju da je upotreba tih tehnologija etična i primerena u obrazovne svrhe i da ne izlaže decu nasilju, diskriminaciji, zloupotrebi njihovih ličnih podataka, komercijalnom iskorišćavanju ili drugim kršenjima njihovih prava, kao što je upotreba digitalne tehnologije za dokumentovanje dečje aktivnosti i deljenje sa roditeljima ili staraocima bez detetovog znanja ili pristanka.

104. Države ugovornice treba da osiguraju da se digitalna pismenost predaje u školama, kao deo programa osnovnog obrazovanja, od predškolskog nivoa i tokom svih godina školovanja, i da se te pedagogije procenjuju na osnovu njihovih rezultata.⁵² Nastavni programi treba da obuhvate znanje i veštine za sigurno rukovanje širokim spektrom digitalnih alata i resursa, uključujući one koji se odnose na sadržaj, stvaranje, saradnju, učešće, socijalizaciju i građanski angažman. Nastavni programi takođe treba da uključuju kritičko razumevanje, smernice o tome kako pronaći pouzdane izvore informacija i identifikovati dezinformacije i druge oblike pristrasnog ili lažnog sadržaja, uključujući pitanja seksualnog i reproduktivnog zdravlja, ljudska prava, kao i prava deteta u digitalnom okruženju i dostupne oblike podrške i korektivnih mera. Države ugovornice treba da promovišu svest kod dece o mogućim negativnim posledicama izloženosti rizicima koji se odnose na sadržaj, kontakt, ponašanje i ugovaranje, uključujući sajber-agresiju, trgovinu ljudima, seksualno iskorišćavanje i zloupotrebu i druge oblike nasilja, kao i strategije za smanjenje štete i strategije za zaštitu ličnih podataka i podataka drugih i da razvijaju socijalne i emocionalne veštine i prilagodljivost dece.

105. Sve je značajnije da deca steknu razumevanje digitalnog okruženja, uključujući njegovu infrastrukturu, poslovne prakse, pouzdane strategije i upotrebu automatizovane obrade i ličnih podataka i nadzora, kao i moguće negativne efekte digitalizacije na društva. Nastavnici, posebno oni koji se bave obrazovanjem o digitalnoj pismenosti i obrazovanjem o seksualnom i reproduktivnom zdravlju, treba da budu obučeni o zaštitnim merama koje se odnose na digitalno okruženje.

B. Pravo na kulturu, razonodu i igru

106. Digitalno okruženje promovise pravo dece na kulturu, razonodu i igru, što je neophodno za njihovo blagostanje i razvoj.⁵³ Deca svih starosnih grupa izjavila su da su doživela zadovoljstvo, interesovanje i opuštanje baveći se širokim spektrom digitalnih proizvoda i usluga po svom izboru,⁵⁴ ali da su zabrinuta što odrasli možda ne razumeju važnost digitalne igre i kako se ona može deliti sa prijateljima.⁵⁵

107. Digitalni oblici kulture, rekreacije i igre treba da podržavaju i koriste deci i odražavaju i promovisu različite identitete dece, posebno njihove kulturne identitete, jezike i nasleđe. Oni mogu olakšati deci socijalne veštine, učenje, izražavanje, kreativne aktivnosti, poput muzike i umetnosti, kao i osećaj pripadnosti i zajedničke kulture.⁵⁶ Učešće u kulturnom životu na mreži doprinosi kreativnosti, identitetu,

⁵²Opšti komentar br. 20 (2016), para. 47.

⁵³Opšti komentar br.17 (2013), para. 7.

⁵⁴“Our rights in a digital world”, s. 22.

⁵⁵Opšti komentar br.17(2013), para. 33.

⁵⁶Isto, para. 5.

socijalnoj povezanosti i kulturnoj raznolikosti. Države ugovornice treba da obezbede da deca imaju priliku da slobodno vreme koriste za eksperimentisanje sa informacionim i komunikacionim tehnologijama, izražavanje i učestvovanje u kulturnom životu na mreži.

108. Države ugovornice treba da regulišu i daju smernice za profesionalce, roditelje i staraoce i da saraduju, prema potrebi, sa dobavljačima digitalnih usluga kako bi se osiguralo da se digitalne tehnologije i usluge namenjene deci, kojima ona pristupaju ili koja na njih imaju uticaj u njihovo slobodno vreme, dizajniraju, distribuiraju i koriste na načine koji poboljšavaju mogućnosti dece u vezi kulture, rekreacije i igre. To može uključivati podsticanje inovacija u digitalnim igrama i srodnim aktivnostima koje podržavaju dečju autonomiju, lični razvoj i uživanje.

109. Države ugovornice treba da osiguraju da se promocija mogućnosti u vezi kulture, razonode i igre u digitalnom okruženju uravnoteži sa pružanjem atraktivnih alternativa na fizičkim lokacijama gde deca žive. Deca, naročito u ranim godinama, uče jezik, koordinaciju i socijalne veštine i stiču emocionalnu inteligenciju uglavnom kroz igru koja uključuje fizički pokret i direktnu interakciju licem u lice sa drugim ljudima. Za stariju decu igra i rekreacija koja uključuje fizičke aktivnosti, timske sportove i druge rekreativne aktivnosti na otvorenom možedoneti zdravstvene pogodnosti, kao i funkcionalne i socijalne veštine.

110. Slobodno vreme provedeno u digitalnom okruženju može decu izložiti rizicima od štete koja može nastati, na primer, usled netransparentnog ili obmanjujućeg oglašavanja ili dizajna koji je posebno uverljiv ili ima kockarske karakteristike. Uvođenjem ili korišćenjem zaštite podataka, privatnosti-po-dizajnu i sigurnosti-po-dizajnu i drugih regulatornih mera, države ugovornice treba da obezbede da preduzeća ne ciljaju decu koristeći pomenute ili druge tehnike dizajnirane da daju prioritet komercijalnim interesima nad interesima deteta.

111. Tamo gde države ugovornice ili preduzećadaju smernice, kao i ocene prema uzrastu, obeležavaju ili sertifikuju određene oblike digitalnih igara i rekreacije, formulacije treba da budu takve da deci ne umanjuju pristup digitalnom okruženju u celini ili da im ometaju mogućnosti za razonodu ili njihovo druga prava.

XII. Posebne mere zaštite

A. Zaštita od ekonomskih, seksualnih i drugih oblika eksploatacije

112. Decu treba zaštititi od svih oblika eksploatacije štetnih za bilo koji aspekt njihove dobrobiti u odnosu na digitalno okruženje. Do eksploatacije može doći u mnogim oblicima, poput ekonomske eksploatacije, uključujući dečji rad, seksualno iskorišćavanje i zloupotrebu, prodaju, trgovinu i otmicu dece i vrbovanje dece za učešće u kriminalnim aktivnostima, uključujući oblike sajber-kriminala. Stvaranjem i deljenjem sadržaja deca mogu postati ekonomski akteri u digitalnom okruženju, što može rezultirati njihovom eksploatacijom.

113. Države ugovornice trebalo bi da preispitaju relevantne zakone i politike kako bi osigurale da su deca zaštićena od ekonomskog, seksualnog i drugih oblika eksploatacije i da su zaštićena njihova prava u vezi sa radom u digitalnom okruženju i odgovarajućemogućnosti za naknadu.

114. Države ugovornice treba da osiguraju postojanje odgovarajućih mehanizama za sprovođenje zakona i da podržavaju decu, roditelje i staraoce u pristupu primenjivoj

zaštiti.⁵⁷ Trebalo bi doneti zakone kako bi osigurali da deca budu zaštićena od štetne robe, poput oružja ili droge, ili usluga poput kockanja. Treba koristiti snažne sisteme za proveru uzrasta kako bi se deca sprečila da pristupe proizvodima i uslugama čije je vlasništvo ili korišćenje od strane dece protivzakonito. Takvi sistemi treba da budu u skladu sa zahtevima za zaštitu i sigurnost podataka.

115. Uzimajući u obzir obaveze država da istražuju, procesuiraju i kažnjavaju trgovinu ljudima, uključujući radnje u vezi s tim i s tim povezano ponašanje, države ugovornice treba da razviju i ažuriraju zakonodavstvo za borbu protiv trgovine ljudima tako da zabranjuju tehnološko olakšavanje regrutovanja dece od strane kriminalnih grupa.

116. Države ugovornice treba da osiguraju da postoji odgovarajuće zakonodavstvo koje štiti decu od zločina koji se dešavaju u digitalnom okruženju, uključujući prevare i krađu identiteta, i da izdvoje dovoljno resursa kako bi se osiguralo da se zločini u digitalnom okruženju istražuju i procesuiraju. Države ugovornice takođe treba da zahtevaju poštovanje visokih standarda sajber-bezbednosti, privatnosti-po-dizajnu i sigurnosti-po-dizajnu digitalnim uslugama i proizvodima koje deca koriste, kako bi se rizik od takvih krivičnih dela sveo na minimum.

B. Izvršenje pravde za decu

117. Za decu se može tvrditi da krše zakone o sajber-kriminalu, ona se za to mogu optužiti ili se to može utvrditi. Države ugovornice treba da osiguraju da kreatori politike razmotre efekte takvih zakona na decu, da se usredsrede na prevenciju i ulože sve napore u stvaranje i korišćenje alternativna krivičnom pravosuđu.

118. Seksualni materijal koji deca sama generišu, a koji poseduju i/ili dele uzspostveni pristanak i isključivo za sopstvenu privatnu upotrebu ne bi trebalo kriminalizovati. Treba stvoriti kanale prilagođene deci kako bi se deci omogućilo da bezbedno traže savet i pomoć kada je u pitanju sopstveni seksualno eksplicitni sadržaj.

119. Države ugovornice trebalo bi da osiguraju da se digitalne tehnologije, nadzorni mehanizmi, poput softvera za prepoznavanje lica, kao i profilisanje rizika, koji se koriste u prevenciji, istrazi i gonjenju zločina ne koriste za nepravedno ciljanje dece osumnjičene ili optužene za krivična dela, niti da se koriste na način koji krši njihova prava, posebno njihova prava na privatnost, dostojanstvo i slobodu udruživanja.

120. Komitet prepoznaje da, tamo gde digitalizacija sudskih postupaka ima za posledicu odsustvo ličnog kontakta sa decom, to može imati negativan uticaj na rehabilitacione i restorativne mere pravde, koje se grade kroz razvoj odnosa sa detetom. U takvim slučajevima, a takođe i tamo gde su deca lišena slobode, države ugovornice treba da obezbede lične kontakte kako bi se deci olakšala mogućnost smislenog stupanja u kontakt sa sudovima i učestvovanja u sopstvenoj rehabilitaciji.

C. Zaštita dece u oružanom sukobu, dece migranata i dece u drugim osetljivim situacijama

121. Digitalno okruženje može deci koja žive u osetljivim situacijama, uključujući decu u oružanom sukobu, interno raseljenu decu, decu migrante, decu koja traže azil i izbeglice, decu bez pratnje, decu prepuštenu ulici i decu pogođenu prirodnim katastrofama, omogućiti pristup informacijama od životnog značaja, koje su ključne za njihovu zaštitu. Digitalno okruženje im takođe može omogućiti da održavaju kontakt sa porodicama, omogućiti im pristup obrazovanju, zdravlju i drugim osnovnim uslugama

⁵⁷Opšti komentar br. 16 (2013), para. 37.

i omogućiti im da dobiju hranu i sigurno sklonište. Države ugovornice treba takvoj deci da obezbede siguran, bezbedan, privatn i koristan pristup u digitalno okruženje i da ih zaštite od svih oblika nasilja, eksploatacije i zloupotrebe.

122. Države ugovornice treba da osiguraju da se deca kroz digitalno okruženje regrutuju i ne koriste u sukobima, uključujući oružane sukobe. To uključuje sprečavanje, kriminalizovanje i sankcionisanje različitih oblika uspostavljanja i negovanja odnosasa decom uz pomoć tehnologije, na primer, korišćenjem platformi za društvene mreže ili usluga časkanja u okviru igara na mreži.

XIII. Međunarodna i regionalna saradnja

123. Prekogranična i transnacionalna priroda digitalnog okruženja zahteva snažnu međunarodnu i regionalnu saradnju, kako bi se osiguralo da sve zainteresovane strane, uključujući države, preduzeća i druge aktere, efikasno poštuju, štite i ispunjavaju prava deteta u odnosu na digitalno okruženje. Stoga je od vitalne važnosti da države ugovornice saraduju bilateralno i multilateralno sa nacionalnim i međunarodnim nevladinim organizacijama, agencijama Ujedinjenih nacija, preduzećima i organizacijama specijalizovanim za zaštitu dece i ljudska prava u vezi sa digitalnim okruženjem.

124. Države ugovornice treba da promovišu i doprinose međunarodnoj i regionalnoj razmeni stručnosti i dobrih praksi i uspostave i promovišu izgradnju kapaciteta, resurse, standarde, propise i zaštitu preko nacionalnih granica, koji omogućavaju ostvarivanje prava deteta u digitalnom okruženju od strane svih država. One treba da podstiču formulisanje zajedničke definicije onoga što predstavlja zločin u digitalnom okruženju, uzajamnu pravnu pomoć i zajedničko prikupljanje i razmenu dokaza.

XIV. Širenje

125. Države ugovornice treba da osiguraju da se ovaj opšti komentar što više širi, što uključuj i upotrebu digitalnih tehnologija, do svih relevantnih zainteresovanih strana, posebno parlamenata i državnih vlasti, uključujući one odgovorne za međusektorsku i sektorsku digitalnu transformaciju, kao i do pripadnika pravosuđa, poslovnih preduzeća, medija, civilnog društva i šire javnosti, prosvetnih radnika i dece, i da bude dostupan u više formata i na više jezika, uključujući i verzije prilagođene uzrastu.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

316.624-053.2:004.738.5(082)

342.726-053.2(082)

364.632-053.2:004.738.5(082)

343.62-053.2(082)

INTERNATIONAL Scientific Thematic Conference Children and the Challenges of the Digital Environment (2022 ; Palić)

Thematic conference proceedings of international significance / International Scientific Thematic Conference Children and the Challenges of the Digital Environment, Palić, 16-17 June 2022. ; [organized by] Institute of Criminological and Sociological Research ; [editors Ivana Stevanović, Milica Kolaković-Bojović]. - Belgrade : Institute of Criminological and Sociological Research, 2022 (Beograd : Pekoграф). - 254 str. : graf. prikazi., tabele ; 24 cm

Tiraž 300. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad. - Rezimeji. - Sadrži i: General comment No. 25 (2021) on children's rights in relation to the digital environment = Opšti komentar br. 25 (2021) o pravima deteta u vezi sa digitalnim okruženjem.

ISBN 978-86-80756-48-6

а) Дигиталне комуникације -- Насиље -- Зборници б) Насиље -- Интернет -- Превенција -- Зборници в) Жртве насиља -- Деца -- Заштита -- Зборници г) Права детета -- Зборници

COBISS.SR-ID 67157001