
Characteristic Forms of Child Abuse on the Internet

Siniša S. Domazet, Slavica S. Dinić and Emil M. Turković
Faculty of Security Studies, Educons University,
Sremska Kamenica, Serbia

Article Information*

Review Article • UDC: 343.62-053.2:004.738.5
Volume: 20, Issue: 3, pages: 179–194
Received: September 15, 2023 • Accepted: October 17, 2023
<https://doi.org/10.51738/Kpolisa2023.20.3r.179ddt>

Author Note

Siniša S. Domazet  <https://orcid.org/0000-0002-5964-2249>

Slavica S. Dinić  <https://orcid.org/0000-0002-7775-8472>

Emil M. Turković  <https://orcid.org/0009-0009-5753-7208>

We have no known conflict of interest to disclose.

Corresponding author: Slavica Dinić

E-mail: slavicadinic@yahoo.com

* Cite (APA):

Domazet, S. S., Dinić, S. S., & Turković, E. M. (2023). Characteristic Forms of Child Abuse on the Internet. *Kultura polisa*, 20(3), 179–194, <https://doi.org/10.51738/Kpolisa2023.20.3r.179ddt>



© 2023 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract

Today's life is characterized by an extremely accelerated development of information and communication technologies. This technical-technological phenomenon, like any other phenomenon, has both positive and negative social implications. Its positive aspects are well-known and are inevitably indisputable. However, as we mentioned, it also has negative sides. Within this work, the subject of analysis will be only one aspect of the negative side of the presence of information and communication technologies in today's society, i.e. we will deal with the issue of the negative impact of information and communication technologies on one of the most vulnerable groups of our society - children. In this sense, we will analyze the international regulations that regulate the issue of child abuse on the Internet. When it comes to domestic regulations, the subject of the analysis will be focused on four characteristic forms of abuse of children on the Internet (trafficking, peer violence, so-called sexual deviations and theft of personal data), and within the framework of normative regulations that combat them, although above all they prevent such phenomena.

Keywords: internet networks, abuse of children, peer violence in the virtual space, child trafficking, sexual deviations towards children in the virtual space, theft of children's personal data on the Internet

Characteristic Forms of Child Abuse on the Internet

Introduction

In the era of accelerated development of modern information and communication technologies, increasing abuses on the Internet are noticeable, and especially the youngest fellow citizens, that is, children, are affected by negative phenomena. According to Vesic and Bjelajac, “in addition to the tremendous technological opportunities available to individuals, organizations and society as a whole, many threats evolve and are transferred in a more or less different form to the digital world until the consequences do not disappear. High technological dependence blurs the line between the virtual and the real” (Vesić & Bjelajac, 2023).

Children are spending an increasing amount of time online. While the internet offers opportunities and potential for expanding horizons and fostering creativity worldwide, it also brings significant risks (See more: Bjelajac & Filipović, 2021; Bjelajac, 2012). Various forms of digital violence can harm the psychophysical health of children and turn them into traumatized victims. Therefore, the importance of promoting internet security culture is increasingly emphasized (See more: Bjelajac & Jovanović, 2013). As the problem of child abuse on the internet takes on increasingly serious proportions, governments worldwide are making efforts to combat these negative phenomena. The problem of child abuse on the Internet is taking on increasingly serious proportions, so governments around the world are trying to suppress these negative phenomena. In this sense, on April 27, 2016, the European Parliament and the Council of the European Union adopted a regulation on the protection of natural persons (especially children) in relation to the processing of personal data and on the free movement of such data. The provisions of the mentioned decree concerning the protection of children in this sphere will be analyzed in the continuation of the work. Also, the legislative body of the Republic of Serbia, by passing various types of legal regulations, makes efforts to protect children from abuse on the Internet. The regulations adopted by the Republic of Serbia in order to protect children from four characteristic forms of abuse on the Internet

(trafficking, peer violence, so-called sexual deviations and theft of personal data) will be analyzed in the second part of this paper.

Bearing in mind the fact that children are a very vulnerable group, it is surprising that children are the fastest growing group of victims of identity theft. In the United States alone, 500,000 children fall victim to identity theft each year. Based on a Carnegie Mellon University Sailab study of 40,000 children, children are 51 times more likely to be victims of identity theft than adults (Goodman, 2017, p. 150). According to the National Crime Prevention Council (in the USA, see authors), almost half of all teenagers are affected by cyberbullying, i.e. a form of peer violence. For young people facing persistent bullying, it seems to work out, and as a result, as many as 20 percent of high school students have admitted to seriously considering suicide due to online bullying (Goodman, 2017, pp. 151–152).

It is inevitable that we have to point out that video games are also a significant problem today. Of course, we cannot dispute the positive aspects of video games, such as: development of the child's perception and intellectual abilities, development of problem-solving skills, improvement of memorization of information, improvement of the ability to draw conclusions, and positive influence on the child's mood. However, there are also risks that children can face. This primarily refers to creating an addiction to video games (in 2018, the World Health Organization classified video game addiction as an addictive disease), which can result in problems for the child with satisfying his biological needs (nutrition, sleep), fulfilling school obligations, and difficulties with establishing and maintaining social interactions. Also, establishing an interaction with other players, often people unknown to the child, can have a risk for the child. In addition to the above, the particular threat of video games is reflected in the fact that a large number of them contain scenes of often even extreme violence, explicit content of a sexual nature, then scenes of drug consumption, gambling, which is especially problematic if we know that children often imitate what they see. So, "Video games are undeniably a very influential segment of ICT, but, as a sort of antipode, social institutions have expressed concerns regarding the potential destructive impact of violent video games on aggression and behavior of individuals" (Filipović, 2023, p. 63).

Playing video games often involves spending money, which, in addition to the known negative aspects, also includes the possibility of data theft.

As we have already stated, this paper will analyze the characteristic forms of abuse of children on the Internet, where the emphasis will be placed on trafficking, peer violence, theft of personal data, as well as the so-called sexual deviations. At the same time, the first part of the paper will discuss the most important international regulations governing the rights of children on the Internet, and the second part of the paper will focus on the regulations adopted by the Republic of Serbia in order to protect children from four mentioned characteristic forms of abuse on the Internet. The research used the normative method, as well as the legal-logical methods of induction and deduction.

International legal regulation regarding children's rights on the Internet

In addition to the Convention on the Rights of the Child, which recognizes the child's right to informational privacy, special reference should be made to Regulation 2016/679 of the European Parliament and the Council of the European Union on the protection of natural persons in relation to the processing of personal data and on the free movement of such data and on repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter: GDPR. In the earlier Directive 95/46/EC did not regulate the issue of children's rights on the Internet in any way, so the provisions that apply to adults also applied to children. Things started to change only in 2006, when the European Commission adopted the corresponding Strategy on the Rights of the Child, in which it emphasized the priority importance of the rights of the child (Commission of the European Communities, 2006). After that, a special advisory working group composed of representatives of national bodies for the protection of personal data expressed the opinion that the processing of children's personal data requires special protection (Lievens & Verdoodt, 2018, p. 270).

Unlike the previous Directive, the new Regulation deals with the rights of children in the most direct way in connection with the protection

of personal data. Thus, Recital 38 of the GDPR states that children, according to their characteristics, must have special protection when it comes to the processing of their personal data, and especially when it comes to the use of such data “for the purposes of marketing or maintaining the profile of the user’s personality and collecting personal data related to children when using services that are offered directly to the child” (Regulation (EU) 679/2016, recital 38).

However, recital 75 of the GDPR states that as a consequence of the processing of personal data, there may be a risk to the rights and freedoms of physical persons, which may manifest itself in the form of “physical, material or non-material damage” (Regulation (EU) 679/2016, recital 75). However, the next, i.e. recital 76. GDPR it talks about the likelihood of a risk to the rights and freedoms of a person, as well as the degree of that risk, and it is stated that this risk depends on the nature, scope, context and purpose of data processing (Regulation (EU) 679/2016, recital 76).

The GDPR, unlike the UN Convention on the Rights of the Child, does not contain a definition of “child”, which is a serious drawback, because by interpreting its provisions it cannot be concluded which protective rights contained in recital 38 of the GDPR actually refer to children. This should be interpreted in such a way as to apply the solution of the UN Convention on the Rights of the Child, which provides for an age limit of up to 18 years. There was also criticism of this solution, some of which referred to the fact that such a solution puts older minors (for example, 13 or 16 to 18-year-olds) in an unequal position (Lievens & Verdoodt, 2018, p. 270)). In other words, it can be argued that, by applying a fixed age limit, the GDPR does not offer children, at least in the age group up to 16, an adequate opportunity to experiment as autonomous persons, as it does not take into account the development of children’s capacities (Buitelaar, 2018, p. 300).

Particular attention should be paid to the rights of the child to Articles 6(1)(a) and 8 of the GDPR. Pursuant to Article 6(1)(a) GDPR, processing shall be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes (Regulation (EU) 679/2016, Art. 6(1)(a)). Article 8 of the GDPR states that personal data can be processed if it is a person who has reached

the age of 16, otherwise, the consent of the person who has parental responsibility for the child is required. However, even under this condition, the age of the child cannot be below 13 years (Regulation (EU) 679/2016, Art. 8).

Article 25 of the GDPR talks about technical and organizational measures that the controller undertakes when planning the processing, and especially during the processing of personal data itself. Accordingly, it is expressly emphasized that only personal data that are necessary for each specific purpose of processing are processed, taking into account their quantity, scope of processing, storage period and availability (Regulation (EU) 679/2016, Art. 25).

This provision is significant, as it allows companies to access children's personal data relatively easily. In this regard, it is easy to imagine a situation where children (or their parents or guardians) usually give their personal information on social networks, without thinking much about the consequences of such a decision. Therefore, children's consent is required, but with the provision of appropriate mechanisms (with mandatory consideration of the child's psychological specifics), which would ensure that children fully understand how their data is managed.

The GDPR rules on the right to delete data ("the right to be forgotten") are particularly important for children's rights, which are mentioned in recital 65 of the GDPR. It is the possibility that at the request of the person who provided their personal data, they can be changed or deleted. In addition, it is particularly significant and the part of this provision that refers to the right to delete data in case of illegal processing of personal data, or on the basis of information society service offers, is particularly significant. This is important for the rights of children, given that they are not aware of all the possibilities of processing their data, especially in the light of blockchain technologies. The controller would have to inform the data processors that the data holder (who is an adult at that time) has requested their deletion, and it is necessary for them to delete personal data from their databases. This is, however, very difficult to implement when the data is processed for the purposes of profiling or marketing campaigns. Then the data holders are not even aware that their data is being processed, especially taking

into account the scandal related to the company Cambridge Analytica and the big affair related to the misuse of personal data of citizens around the world (Domazet & Skakavac, 2016, p. 71), and also children.

Characteristic forms of child abuse on the Internet from the aspect of the legal regulations of the Republic of Serbia

Examples of child abuse on the Internet are numerous and varied. However, for the purposes of analysis within this work, we will focus on four characteristic forms of child abuse on the Internet: trafficking, peer violence, so-called. sexual deviations and the theft of personal data, and within the framework of the normative regulations that suppress them, although above all they prevent such phenomena.

Theft of personal data

One of the most common forms of abuse of children on the Internet is related to the theft of their personal data, i.e. the so-called phishing. Children have been shown to be very vulnerable to this form of cybercrime. In recent years, phishing attacks targeting children have increased dramatically with the rise of very young Internet users (Alwanain, 2021, p. 128). In the initial stages of the development of phishing, perpetrators used relatively simple fraud methods, so that phishing emails were relatively easy to recognize (for example, they contained numerous grammatical and spelling errors), while today phishing has evolved and become much more complex and sophisticated, including the use numerous advanced software solutions for concealment in order to obtain sensitive (personal) data (Domazet & Skakavac, 2019, p. 191). In particular, financial fraud is apostrophized, as one of the biggest cyber threats for children (Vodafone UK News Centre, 2021).

The Criminal Code of the Republic of Serbia sanctions the theft of personal data under Article 146, which criminalizes the unauthorized collection of personal data. The object of protection of this incrimination are the freedoms and rights of man and citizen. The crime has three forms. First, the form sanctions the unauthorized acquisition, disclosure and use of personal data that is collected, processed and used on the

basis of the law. In the event that these data are collected against the law and used as such, elements of another form of being of this criminal offense will be realized. If the first form of this criminal offense is committed by an official, it will be its third qualified form.

The protection of personal data is also guaranteed by the Constitution of the Republic of Serbia, in Art. 42, i.e. the highest legal act. Also, the Law on the Protection of Personal Data is fully devoted to this issue.

Sexual deviations (Sexual violence on the Internet)

Children, very simply, and thus very often, become victims of sexual violence on the Internet. As is generally known, insufficient psychological development contributes to this, which, after a child becomes a victim of this type of violence, has a further, deeper destructive effect on that same child. Namely, when children find themselves in this problem, they often see the only way out is to take their own life.

How dangerous this phenomenon is for an individual (specifically a child victim of sexual violence on the Internet), the child victim's family, and of course, the entire society, it is clear to us even if we have just "started" this topic. The legislator of the Republic of Serbia, with the aim of primarily preventing, but also suppressing, among other things, this type of violence against children on the Internet, prescribes two incriminations (National Assembly of the Republic of Serbia, 2019, Art. 185 and 185b).

The first indictment sanctions the display, acquisition and possession of pornographic material and the exploitation of a minor for pornography (National Assembly of the Republic of Serbia, 2019, Art. 185). Being the first form of this incrimination sanctions making pornographic material available to a minor, i.e. a child (the third qualified form of this criminal act). The second (serious) form of this criminal offense sanctions the exploitation of minors for the production of pornographic material, and if the object of the action is not a minor but a child, there will be a third qualified form of this criminal offense. The act of the fourth form will be carried out in the event that the

pornographic material created in this way is acquired for oneself or another, possessed, or generally made available. The fifth form of this incrimination will exist if, with the help of information technologies, pornographic material created by the exploitation of minors is consciously accessed. The term “child pornography” means “any material that visually depicts a minor engaging in real or simulated sexually explicit behavior, as well as any depiction of a child’s sexual organs for sexual purposes” (National Assembly, 2019, Art. 185).

In connection with the issue of sexual violence against children on the Internet, the legislator criminalizes the use of a computer network or communication by other technical means to commit crimes against sexual freedom against a minor (National Assembly, 2019, Art. 185b). The existence of this incrimination, related to the issue of sexual violence against children on the Internet, exists in the event that someone “using a computer network or communication by other technical means arranges a meeting with a minor and appears at the agreed place for the purpose of the meeting” and in order to commit one of the criminal offenses from the group against sexual freedom.

Human Trafficking

Almost anyone can become a victim of trafficking (trafficking in human beings) today, especially a child. Everyone who chats online, leaves photos and expresses their views on social networks is at risk. According to some data, “the victims are mostly female, aged between eleven and twenty-five”¹. On the other hand, human traffickers are not easy to trace, on the contrary. They are well organized, have globally developed networks, which is logical because it is a very lucrative business, while on the other hand, they can even “be in contact with the victim for several years in order to gain her trust”, in which case they “success” almost guaranteed.

¹ According to the law of the Republic of Serbia, a person who has not reached the age of fourteen is considered a child. A minor is a person who has reached the age of fourteen, but has not reached the age of sixteen. A person who has reached the age of sixteen and has not reached the age of eighteen is an older minor.

The Republic of Serbia, in order to prevent such phenomena, but also to suppress them, criminalizes human trafficking (National Assembly of the Republic of Serbia, 2019, Art. 388). The first form of this criminal offense is committed by "who, by force or threat, misleading or maintaining a delusion, abuse of authority, trust, dependence, difficult circumstances of another, withholding personal documents or giving or receiving money or other benefits, recruits, transports, transfers, hands over, sells, buys, mediates the sale, hides or keeps another person, and with the aim of exploiting his work, forced labor, committing criminal acts, prostitution or other types of sexual exploitation, begging, use for pornographic purposes, establishing a slave or similar relationship, for the removal of organs or parts of the body or for use in armed conflicts. The second form of this offense exists when the first form is committed against a minor, completely unrelated to the method of execution. The third form exists in the situation when the first form of the act (including the prescribed act of its execution) is committed against a minor. The fourth form exists in the event that the execution of the first, second or third form of the act resulted in serious physical injury to a minor. In the event that the death of one or more persons occurs as a result of the execution of the offense from the first and third form, there will be a fifth form of this criminal offense. The sixth form exists in the event that someone engages in the first, second or third form of this criminal offense, or if the offense was committed by a group. The seventh form exists if the first, second or third form was committed by an organized criminal group. The eighth form of the offense will exist in the event that someone "knows or could have known that a person is a victim of human trafficking, so he takes advantage of her position or allows someone else to take advantage of her position for the purpose of exploitation provided for" by the first form of this criminal offense. The ninth form exists in the event that the act from the eighth form is "committed against a person whom the perpetrator knew or could have known was a minor." The tenth form of this criminal offense excludes the consent of the person (victim) "to exploitation, or to the establishment of a slave or similar relationship" which provides for the first form of the offense, in the sense that this consent will not affect the existence of the first, second and sixth forms of the criminal offense of human trafficking.

Peer violence

Unfortunately, like the previous three forms of child abuse on the Internet, this one is not at all harmless. Namely, the violent behavior of children on the Internet (in the digital world) is much more dangerous than that which is carried out in the classic form (in the real world), because the victim is first of all constantly (24 hours) exposed to violence. Second, the abuser has no real insight into the victim's suffering, but only an assumed one, which often results in the continuation and intensification of violence by the abuser towards the victim. The consequences for the victim of this type of violence are often disastrous.

And the legislator of the Republic of Serbia tries to prevent (but, when there is a need for it, suppress it), by criminalizing violent behavior (National Assembly of the Republic of Serbia, 2019, Art. 344). This incrimination has two forms. The first, basic form will exist if someone "by grossly insulting or abusing another, committing violence against another, causing a fight, or by insolent or reckless behavior significantly endangers the tranquility of citizens or more seriously disturbs public order and peace." The second, qualified form of this criminal offense will exist if the basic form of this criminal offense was committed "in a group, or during the execution of the offense, a minor physical injury was inflicted on a person, or there was serious humiliation of citizens."

Conclusion

The issue of child abuse on the Internet is therefore not harmless, and it is not a rare phenomenon either. We can look for the reason for this in the level of insufficient psychological maturity of the child. However, this is a well-known, unchangeable fact that the legislator also recognized, and considers a person who has reached the age of eighteen to be an adult. But, as psychological maturity does not occur in every individual upon reaching this number of years of life, the law also recognizes the category "younger adult" (a person who has reached the age of eighteen and not reached the age of twenty-one).

Accordingly, it is clear that we cannot change the biological basis, but first of all we must focus on the social aspect of protecting this very

vulnerable category of the human community. Therefore, it is necessary to establish legal mechanisms for the protection of children on the Internet, i.e. in the so-called virtual space. We can state that on the international, as well as the national level, legal regulation is relatively well established. Another issue is its application, ie. implementation. Namely, this issue was not the subject of our analysis, but it is a well-known fact that the community of European nations, as well as the institutions of our country, make extraordinary efforts in implementing the regulations that regulate this area. As it is a relatively new phenomenon in our society (the mass use of the Internet in our country only dates back to 2008), it is logical to encounter difficulties in its prevention and suppression. In addition to legal regulations, we consider strengthening the social ties of children and minors, first of all with the family, but also with the environment, of extreme importance, above all for the prevention of this phenomenon, which is important because the closest environment of the child, if he has developed trust in the same, can in time recognize the problem that the child has or the possibility of the child getting into a problem. In addition to legal regulations, the family, the close environment of the child, which are extremely important in the prevention of abuse of children on the Internet, and the remediation of its consequences, it is necessary to include professional services. The synergy of all the above can certainly significantly improve the situation in this field.

References

- Alwanain, I M. (2021). How do children interact with phishing attacks? *International Journal of Computer Science and Network Security*, 21(3), 120-139.
- Bjelajac, Ž. (2012). Cyber crime and internet pedophilia as an important international phenomenon. In: *Western Balkans: From Stabilization to Integration*. The Institute for International Politics and Economics, 437–456.
- Bjelajac, Ž., & Jovanović, M. (2013). Pojedini aspekti bezbedonosne kulture na Internetu [Certain Aspects of Internet Security Culture]. *Kultura polisa*, 10(21), 99–114.

- Bjelajac, Ž., & Filipović, A. (2021) Fleksibilnost digitalnih medija za manipulativno delovanje seksualnih predatora [Flexibility of digital media for manipulative activities of sexual predators]. *Kultura polisa*, 18(44), 51–67.
- Buitelaar, J.C. (2018). Child's best interest and informational self-determination: what the GDPR can learn from children's rights. *International Data Privacy Law*, 8(4), 298–311.
- Commission of the European Communities (2006, July 4). *Towards an eu strategy on the rights of the child*. Commission of the European Communities. COM(2006) 367 final.
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0367&from=NL>
- Domazet, S., Skakavac, Z. (2019). "Phishing" – a challenge in protecting the data security of internet users. *Serbian political thought*, 63(1), 183–199.
- Domazet, S., Skakavac, Z. (2016). "Right to be forgotten" and the general regulation of the european union 2016/679 on the protection of personal data. *European legislation*, 17(66), 65–82.
- Filipović, A. (2023). Possible effects of playing video games with explicit violence on player aggression. *Kultura polisa*, 20(2), 61–81, <https://doi.org/10.51738/Kpolisa2023.20.2r.61f>
- Goodman, M. (2017). *Crimes of the future*. Laguna.
- Lievens, E., Verdoodt, V. (2018). Looking for needles in a haystack: key issues affecting children's rights in the general data protection regulation. *Computer law & security review*, 34(2018), 269–288.
- National Assembly of the Republic of Serbia [National Assembly]. (2021). *Constitution of the Republic of Serbia* [Constitution of the Republic of Serbia]. (Official Gazette of the Republic of Serbia, no. 98/2006 and 115/2021).
- National Assembly of the Republic of Serbia [National Assembly]. (2018). *Personal Data Protection Act* [Personal Data Protection Act]. (Official Gazette of the Republic of Serbia, no. 87/2018).

- National Assembly of the Republic of Serbia [National Assembly]. (2019). *Criminal Code of the Republic of Serbia* [Criminal Code of the Republic of Serbia]. (Official Gazette of the Republic of Serbia, no. 85/2005, 88/2005 – corrected, 107/2005-corrected, 72/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019). <https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html>
- National Assembly of the Republic of Serbia [National Assembly]. (1996). *Law on Ratification of the United Nations Convention on the Rights of the Child* [Law on Ratification of the United Nations Convention on the Rights of the Child]. ("Official Gazette of the SFRY - International Treaties", no. 15/90 and "Official Gazette of the FRY – International Treaties", no. 4/96 and 2/97). http://www.paragraf.rs/propisi_download/zakon_o_ratificationaci_ji_konvencije_ujedinjenih_nacija_o_pravima_deteta.pdf
- Regulation (EU) 679/2016. *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 processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. The European Parliament & the Council of the European Union. Official Journal of the European Union, L 119. <http://data.europa.eu/eli/reg/2016/679/oj>
- Vesić, S., & Bjelajac, M. (2023). Cyberbullying: between the virtual and the real. *Kultura polisa*, 20(2), 82–100. <https://doi.org/10.51738/Kpolisa2023.20.2r.82vb>
- Vodafone UK News Centre (2021, Mar 3). *Why financial scams may be the biggest cyber-threat to your children*. News Centre Vodafone UK. <https://newscentre.vodafone.co.uk/smart-living/digital-parenting/why-financial-scams-may-be-the-biggest-cyber-threat-to-your-children/> (09 12. 2021)

Karakteristični oblici zloupotrebe dece na internetu

Siniša S. Domazet, Slavica S. Dinić i Emil M. Turković
Fakultet za studije bezbednosti Univerziteta Edukons, Sremska
Kamenica, Srbija

Sažetak

Današnjicu karakteriše izrazito ubrzan razvoj informaciono-komunikacionih tehnologija. Ova tehničko-tehnološka pojava, kao u ostalom i svaka druga pojava, ima i pozitivne i negativne društvene implikacije. Njene pozitivne strane dobro su poznate i neizostavno su nesporne. Međutim, ona, kao što smo pomenuli, poseduje i negativne strane. U okviru ovog rada predmet analize biće samo jedan aspekt negativne strane prisutnosti informaciono-komunikacionih tehnologija u današnjem društvu, tj. bavićemo se pitanjem negativnog uticaja informaciono-komunikacionih tehnologija na jednu od najranjivijih grupa našeg društva – na decu. U tom smislu, analiziraćemo međunarodne propise koji regulišu pitanje zloupotrebe dece na internetu. Kada je reč o domaćoj regulativi predmet analize biće fokusiran na četiri karakteristična oblika zloupotrebe dece na internetu (trafiking, vršnjačko nasilje, tzv. seksualne devijacije i krađu ličnih podataka), a u okviru normativnih propisa kojima se suzbijaju, mada pre svega preveniraju ovakve pojave.

Ključne reči: internet mreže, zloupotreba dece, vršnjačko nasilje u virtuelnom prostoru, trafiking dece, seksualne devijacije prema deci u virtuelnom prostoru, krađa ličnih podataka dece na internetu