UDC: 316.624-053.2:004.738.5(100)
DOI: https://doi.org/10.5937/pnb24-44680
Review article

The Policy of National Security
Year XIV, vol. 24
No. 1/2023.
pp. 153-173

Siniša S. Domazet*

Faculty of Security Studies, Educons University, Sremska Kamenica

Ivona Šušak-Lozanovska

Faculty of Law, University St. Kliment Ohridski, Bitola

CHILDREN'S DATA AND PRIVACY ONLINE – GROWING UP IN A DIGITAL AGE

Resume

Adolescents in the age of technology face a variety of security issues, but one of the most significant ones, that needs to be addressed by legislators, is privacy and data protection. Research has shown that children's rights, especially children's privacy, are regulated by a large number of international regulations. At the European level, both the European Union and the Council of Europe guarantee the rights to privacy and data protection. The Children's Online Privacy Protection Act is the relevant act in the US. The most common violations of children's data and privacy have been found to be online data sharing and mobile application data collection practices. Children's privacy on the Internet can be improved by better communication between parents and children regarding Internet use, educating children about cyber security and online threats, using parental control software, installing antivirus programs on devices used by children and the like.

Keywords: Law, Security, Cyberspace, Children, Privacy

* Contact: sdomazetns@gmail.com

INTRODUCTION

The number of young Internet users has increased substantially in recent years, indicating that one-third of all Internet users worldwide are under 18 years old. (UNICEF 2019). The now growing Z (born between 1995-2010.) and Alpha (2010 -) generations has a tendency to spend more time online, and they start living their online life at a younger age.

Technological development offers incredible opportunities and can progress everyday life, but each major advantageous improvement also has many disadvantages. The emergence of internet-connected toys as well as other smart gadgets and applications that weren't necessary created for kids' usage has drawn much criticism. Unfortunately, they added many hidden concerns, such as invasions of privacy and data protection violations, in addition to the obvious risks like becoming a victim of some rather sexual violence, becoming addicted or with low self-esteem, becoming overweight or having other more serious health problems.

As a result children are becoming "data subjects" whose information are shared, gathered, and analyzed without their awareness or any comprehension of the repercussions. (Caglar 2021).

For children raised in a digital world, childhood has become "a critical site of datafication and dataveillance" (Mascheroni 2018). The digitalisation of their "lifeworlds" significantly affects both their ability to exercise their rights and the likelihood that their rights will be upheld or ignored. Because of this, just as every parent teaches their child the fundamental skills, they need knowing, such as exercising caution when crossing the street, it is now crucial for parents to educate their children how to use the Internet responsibly. However, governments also have important duties to carry out to highlight the need for children's protection, not just in their real lives, but also on the Internet.

In the digital era, children face a variety of security issues, but one of the biggest issues that has to be addressed by lawmakers is privacy and data protection. The paper will cover more of these problems and dilemmas.

THE CONCEPT OF THE RIGHT TO PRIVACY

The dynamic development of information and communication technologies, artificial intelligence, blockchain technologies, the Internet

of Things has brought numerous changes in modern society and improved the lives of citizens. As stated by Dimitrijević, "with the development of communication networks, emerged the notion of 'networked society', a virtual world in which everyone communicates with everyone. This communication becomes a source of the most diverse data about people, since in the virtual world a person is far less careful. Apparent invisibility and distance creates a feeling of anonymity and security, so in certain situations people tend to give their personal data or undertake actions they would never do in the physical world" (Dimitrijević 2014.). However, it has been shown that modern technologies can be misused in various ways, especially when it comes to privacy. This opened numerous questions regarding the preservation of guaranteed human rights, but also opened the dilemma of the existing definitions of the concept of privacy. According to Diggelmann and Cleis, "the right to privacy made an impressive international career in the second half of the twentieth century, particularly because the umbrella notion lends itself to an application in diverse fields. In our age of information technology and electronic media, the integral guarantee of a right to privacy became a key right. Secondly, the importance of the right contrasts with the uncertainties about its con-ceptual basis" (Diggelmann / Nicole Cleis 2014). The right to privacy is particularly threatened by phishing, which has "evolved and become much more complex and sophisticated, including the use of numerous advanced software solutions for concealment to obtain sensitive (personal) data" (Autor 2018, 115-133).

At the moment, there is no universally accepted definition of privacy on the international level, but there are many different approaches to this concept in theory and jurisprudence.

For example, Bošković defines the right to privacy as "the right to prevent the risk, or reduce the risk to an acceptable level, that one subject uses other people's private information, without being authorized to do so" (Bošković 2017). The definition of privacy given by American judges Samuel Warren and Louis Brandais in the 19th century is also interesting, who define the right to privacy as "the right to be left alone" (Warren / Brandais 1890). According to Diggelmann and Cleis, „the right to privacy had become an International HR before it was a nationally well-established fundamental right" (Diggelmann / Nicole Cleis 2014). Another definition of the right to privacy that was "born" by American jurisprudence should be mentioned at this point. Thus, in the 1965 case of Griswold v. Connecticut, which was decided before the US Supreme

Court, Sarat said that "the court identified a right to privacy grounded in the 'penumbras' and 'emanations' of the First, Third, Fourth, Fifth, and Ninth Amendments to the US Constitution and argued that the right to privacy in marriage was older than the Bill of Rights itself" (Sarat 2015).

According to Sinđelić, „in the second half of the 20th century, this right grew into the right to personal autonomy and consisted of guaranteeing through legal regulations a sphere of personal autonomy within which each individual would have the right to independently regulate their relations with other people. In France, it functions as a unique notion of private life, understood narrowly and with an emphasis on secrecy. In the German doctrine, the right to privacy was very limited, until a rule in 1954 by the Federal Court recognized the general personal rights, and explicitly the right of every person to a private sphere" (Sinđelić 2012). The same author states that „the Swiss Civil Code contains a general clause on the protection of the individual, which is the legal basis for the protection of the right to privacy. The already determined right to privacy is the absolute subjective right of a natural person to be able to independently decide on introducing third parties to any manifestation of their personal existence. From this right arose specifically personal rights such as: the right to private life, the right to character, the right to vote, the right to personal writings" (Sinđelić 2012).

There is also a definition given by Ho, Hichang, Rivera-Sánchez, Milagros, Lim, Sun Sun, who consider privacy as "personal autonomy, democratic participation, managing one's own identity and social coordination" (Cho, Rivera-Sanchez / Sun Sun 2009) Kurland took the position that the right to privacy represents "a set of three rights: the freedom from intrusion and unauthorized observation of one's private life, the right to maintain control over personal information, and the freedom to act without interference" (Kurland 1976) In the literature, there are viewpoints according to which privacy is defined as a political right, but also as a "right that exists to protect the interests of citizens" " (Barnes 2006). Garfinkel defines the right to privacy as "as having control over something that belongs to the person, their autonomy and integrity, or as their right to control what details of their life can be disclosed" (Garfinkel 2000). There are also authors who understand the right to privacy as "the right of an individual to be protected from intrusion into their personal life, business affairs, lives of their family members, either by direct action or by disclosing personal information" (Shah 2013).

The literature also uses the term "information privacy", which according to Boban, includes "information security, which means that an individual that lives in an information society decides when, to whom, to what extent and how will their personal data be disclosed, taking into account their rights and needs, as well as the rights and needs of the community they live in" (Boban 2012). Also, according to Boban, "information privacy incorporates the legal values of protection of the rights of individuals in a society with developed information technologies, whereas this concept of personal data protection related to communication via electronic networks is also called 'e-privacy'" (Boban 2012). On the other side, there are also authors who use the term "privacy in electronic communications", which includes "collecting, processing and providing information about the user to third parties, whereby individuals when recording activities and personal data determine when, how and in which measures information about their private sphere should and can be available to others" (Jovanović 2014).

When it comes to the right to privacy, it is of the greatest importance to refer to the relevant international regulations, as well as the activity of international organizations.

In this regard, the European Convention on Human Rights (ECHR) in Article 8 provides the "right to respect for one's private and family life, home and correspondence". According to ECHR „the suspension of this right may be exercised only when prescribed by Law or when necessary in a democratic society, in the interest of national security, public safety or economic well-being of the country, to prevent social disorder and crime, to protect public health or morality, or to protect the rights and freedoms of others". The right to privacy is also protected by Article 12 of the UN Universal Declaration of Human Rights from 1948, which states that "no one shall be subjected to arbitrary interference with private life, family, home or correspondence, nor to attacks on honor and reputation." Everyone has the right to the protection of the law against such interference or attack." A similar position is contained in Article 17 of the International Covenant on Civil and Political Rights from 1966, which states that "no one shall be subject to arbitrary or unlawful interference with his private life, his family, his home or his correspondence, nor illegal injuries caused to his honor or his reputation."

When it comes to the UN, General Assembly emphasized that member states had the duty to "respect and protect the right to privacy, including in context of digital communication" (United Nations General

Assembly, The right to privacy in the digital age 2013), and that "the same rights that people have offline must also be protected online, including the right to privacy" (United Nations General Assembly, The right to privacy in the digital age: resolution 2015). The prohibition of violation of the right to privacy is also present in the Commentary of the UN High Commissioner for Human Rights from 1988, where in par. 8. states that "surveillance, whether electronic or otherwise, interception of telephone, telegraphic and other forms of communication, eavesdropping and recording of conversations should be prohibited" (Office of the High Commissioner for Human Rights 1988).

Also, the 2014 Report of the UN High Commissioner for Human Rights also points to the prohibition of violating the right to privacy and points out that "the state must ensure that any interference with the right to privacy, family, home or correspondence is permitted by laws which (a) are publicly available; (b) contain provisions that ensure that the collection, access and use of communication data is tailored to certain legitimate purposes; (c) are sufficiently precise, specifying in detail the precise circumstances in which such interference may be permitted, procedures for granting authorization, categories of persons who may be placed under surveillance, limitations on the duration of surveillance, and procedures for the use and storage of collected data; and (d) provide effective safeguards against abuse" (United Nations General Assembly, The Right to privacy in the Digital Age 2014).

The jurisprudence of the European Court of Human Rights also protects the right to privacy. This was pointed out, for example, in the case of Liberty and Others v. The United Kingdom from 2008, where in par. 56. states that "telephone, fax and e-mail communications are covered by the terms "private life" and "correspondence" in the sense of Article 8 (European Convention on the Protection of Human Rights and Fundamental Freedoms, ed. S.D). The Court recalls its findings in previous cases [...] that the mere existence of a law authorizing a system for the secret monitoring of communications implies a threat of surveillance to all those to whom the law may apply. This threat necessarily affects the freedom of communication between users of telecommunication services and thus represents an interference with the exercise of the rights of the applicants under Article 8, regardless of all the measures taken against them" " (Case of Liberty and Others v. The United Kingdom 2008).

Considering all the complexity of this concept and the challenges brought about by new technologies, it should not be surprising that

various bodies dealing with the protection of human rights have avoided precisely defining the concept of the right to privacy. Moreover, it can be said that in jurisprudence the concept of privacy is understood quite broadly (Author 2022). This was confirmed in the case of Mikulić v. Croatia, where the European Court of Human Rights in par. 54. took the position that "respect for private life requires everyone should be able to determine the details of their identity as individual human beings and that the individual's right to such information is important because of its implications for his personality" (Mikulić v. Croatia Judgment 2002). The position of the Court in the case of Pretty v. is particularly important. United Kingdom. It was underlined there (in par. 61) that "the concept of "private life" is a broad term that is not subject to an exhaustive definition." It covers the physical and psychological integrity of a person. Sometimes it can encompass aspects of an individual's physical and social identity. Elements such as, for example, gender identification, name and sexual orientation and sex life belong to the personal sphere, in accordance with Article 8 (European Convention on the Protection of Human Rights and Fundamental Freedoms, ed. S.D). Article 8 also protects the right to personal development and the right to establish and develop relationships with other human beings and the outside world. Although no previous case has established as such the right to self-determination contained in Article 8 of the Convention, the Court considers the notion of personal autonomy is an important principle underlying the interpretation of its guarantees" (Pretty v. United Kingdom Judgment 2002).

When it comes to national regulations, the right to privacy is regulated differently around the world. Thus, in some countries, the right to privacy is a constitutional category or is indirectly regulated by the constitution, as well as by regulations in the field of criminal legislation (the USA can be taken as an example). Some countries have their own legislation on the protection of personal data (in the Republic of Serbia, it is the Law on the Protection of Personal Data from 2018), while in some countries the right to privacy is unrecognized as an autonomous right at all, as is the case in China (Author 2022, 79-97).

Therefore, in the next part of the paper, we will discuss more about the concept of children's data an privacy online, and then we will move on to the analysis of possible abuses.

CHILDREN'S DATA AND PRIVACY ONLINE – LEGAL PERSPECTIVE

It is obvious that the extensive collection, processing and analysis of personal data has grave consequences for the fundamental rights of data subjects of all age groups. Children deserve special protection due to their particular characteristics, thus they have specialized rights that exclusively apply to them, even though human rights are universal and apply to all equally (Caglar 2021).

The 1989 United Nations Convention on the Rights of the Child (UNCRC) is a significant agreement between nations that committed to defend and uphold children's rights. The UNCRC is an inspirational document that outlines the minimum standards all children should enjoy. According to the UNCRC, "children should be treated with respect and safeguarded, so they can realize their full potential." It also emphasizes the need for adults to behave in children's best interests by protecting them from harm and ensuring their rights are kept safe. (United Nations 1989).

The Convention ensures that every child has the right to privacy, or privacy protection, and also regulates children's access to information. But online existence was not as popular when the UNCRC was established, so no particular regulations regarding online services are included in this text. However, its concepts remain applicable in the virtual as well as the real world. This was confirmed in the UN resolution, which stated unequivocally that "rights that people have offline must also be protected online" (United Nations, UNESCO 2018). The UNCRC's essential principles and cornerstones should guide the stakeholders when implementing current regulations into practice, which consequently removes any question regarding whether these regulations can be used to protect children during the collection and usage of their data.

For a formal clarification of this dilemma, in order to explain how the Convention applies to the digital age, the CRC Committee decided to create a General Comment at the beginning of 2018. On March 24, 2021, General Comment 25 on Children's Rights in Relation to the Digital Environment went into effect, after being formally adopted. It explains, "why and how States and other duty bearers should act to achieve children's rights in the digital age." The CRC Committee is quite aware that discussions about new technologies are polarizing in stating that "the digital environment affords new opportunities for the realization of children's rights, but also poses risks of their violation and

abuse." In few words, when it comes to protecting children's rights in the digital age, the CRC Committee promotes a thoughtful, balanced approach to legislation and policymaking. The best interests of the child should be the first priority, and the development of children's capacities should be a guiding element, in circumstances when public or private actors must strike a balance between child protection and participation (UNCRC 2021).

At the European level, both the Council of Europe (CoE) and the European Union (EU) guarantee the rights to privacy and data protection.

The rights to privacy and data protection are outlined in a number of Council of Europe's documents. These rights, were first of all, guaranteed by article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, following the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The 1981 Convention is the first legally binding international instrument that gives data subjects rights, provides fundamental principles and protections, and defends against abuses that may occur in connection with the collecting and processing of personal data. The Convention was amended in 2018 in light of the shortcomings in data privacy laws. (Council of Europe 2018). The Convention now explicitly compels "institutions to pay close consideration to the rights of children and other vulnerable individuals in data protection when it comes to raising public awareness, given the diverse roles of supervisory authorities" (Štareikė 2022).

Given that all individuals are covered by the ECHR's and Convention 108's provisions, it is obvious that children and adolescents are also covered by these laws and that their privacy and data are protected to the same extent, if not stronger, as those of older generations (ECHR, 2872/02), especially in light of the recent CoE focus on children's rights.

This raising awareness of the importance of protecting children's rights in the complex conditions of digitalization is especially evident through a series of recommendations, declarations, resolutions and strategies as part of so-called soft law. For example, the 2008 Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (Committee of Ministers 2008), the 2014 Recommendation on a Guide to human rights for internet users (Committee of Ministers 2014) and the 2016-2021 Strategy for the Rights of the Child (Council of Europe 2016) have emphasized how important it is to protect children's rights in the world of the internet. The CoE Strategy for the Rights of the Child clearly states the digital world exposes

children to a wealth of opportunities, whether it is through computers, gaming consoles, tablets or smartphones" (Council of Europe 2016). The Strategy also stresses the digital environment has a dual function – on the one hand, it is pointed out that digitalization pose a potential danger of increasing vulnerability of children, while on the other hand, it opens the possibility of strengthening and protecting their rights to freedom of expression, to participation and to education (Milkaite / Lievens 2019).

A Recommendation on Guidelines to Respect, Protect, and Fulfill the Rights of Children in the Digital Environment was released by the Council of Europe in July 2018. With the assistance of this directive, stakeholders will be guided to develop and manage the frequently complicated digital environment. It is crucial to ensure the engagement and safety of children in this setting. Among the various topics covered are the vulnerability and resilience, helplines and hotlines, privacy and data protection, providing child-friendly content tailored to their changing needs, as well as the role and responsibilities of business enterprises. To guarantee that national policies effectively meet advancements in the digital world, the guidelines also urge governments to involve children in decision-making processes (Council of Europe 2018).

When it comes to European Union, the protection of privacy and personal data generally are part of the Charter of fundamental rights of the European Union. "Every individual has the right to respect for his or her private and family life, the inviolability of housing and the confidentiality of communication", according to Article 7 of the European Union's Charter of Fundamental Rights. Article 8 determines the protection of personal data, which states that: "Everyone has the right to the protection of their personal data. Personal data must be properly processed and used only for the purposes for which it was collected, with the subject's consent, or in accordance with other legal justifications specified by law" (Charter of Fundamental Rights of the European Union 2000).

Since 1995, when it comes to the European Union's secondary laws, the Data Protection Directive (DPD) has served as the main legal text governing data protection in EU Member States. The General Data Protection Regulation (GDPR), which took effect in 2018, was adopted by the Council and the Parliament of the European Union in the context of the EU data protection reform because the previous legislation was inevitably out of date given that it was adopted more than 20 years ago.

In the paragraph (38) of its preamble, GDPR says that "Children merit specific protection with regard to their personal data, as they may

be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should be unnecessary in the context of preventive or counseling services offered directly to a child" (GDPR 2016/679).

In simple terms, the GDPR permits the collection of data for particular purposes and the storage of such data for a period of appropriate time, taking into account the duration of use and the principle of data minimization. Children's personal information receives extra protection under GDPR, and data controllers that handle children's information in the course of their business are subject to stricter requirements. Because of the difficult technological balance between service quality and compliance requirements in the areas of security and privacy, this rule serves as both a safeguard for children and a problem for digital service providers (Krasznay, Racz-Nagy / Dora 2020).

The Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), which provides guidelines for the processing of personal data in these sectors, is another segment of the EU's data protection model. In the upcoming years, the e-Privacy Regulation will take the place of this Directive. The Regulation would amend the present laws and provide further protections for users of these services, with the goal of preserving and enhancing privacy and data protection in the sphere of electronic communications (Gesley 2021).

The relevant legislation in the United States is the Children's Online Privacy Protection Act (COPPA), which was enforced by the Federal Trade Commission. Limitations on the collection of children's personally identifiable information, requirements for user-friendly and transparent privacy policies, and the need for verifiable parental consent prior to data collection are some of the key provisions of COPPA, thus providing an opt-in model for the processing of data of children under the age of 13. COPPA took effect in 2000, and in 2012, its regulations were updated to include protections for a mobile, geolocation, gaming, and social media activities. The definition of personally identifiable information was also expanded to include photos and other online content, and behavioral advertising, the use of "cookies," and other identifiers were also restricted.

It's interesting to note the GDPR doesn't go into greater detail about this as the Children Privacy Protection Act does. It offers detailed illustrations and procedures for gaining valid consent. The GDPR now offers strong protections for children's privacy and data protection, but, it still needs to be improved to increase transparency and give individuals control over their personal information. This presents an opportunity to evaluate the current principles and how they are being implemented into practice (Verdoodt, Clifford / Lievens 2016).

MOST COMMON VIOLATION OF CHILDREN'S DATA AND PRIVACY ONLINE

There are many forms of violation of children's rights and violations of children's privacy. With the development of information and communication technologies, the variety and number of infringement cases will increase. Among the most famous forms of violation of children's privacy stand out "Sharenting" and Data Collection Practices of Mobile Applications.

"Sharenting"

"Sharenting" tends to be defined as any situation where an adult "transmits private details about a child via digital channels." Children's information can be uploaded to various data tracking technologies including fertility apps, smart toys or personal cloud servers, even though the phrase "sharenting" is typically used to relate to social media and popular telecommunications channels (Hsu 2019).

Taking adorable or humorous pictures and videos of children is nothing new, almost certainly we have all looked through family photo albums our parents created or seen home videos of ourselves at various ages and stages. However, as childhood and family life become more mediatized (Krotz & Hepp 2011), this leads to an increase in online visualization, which then follows a sharp rise in online photo sharing intended to produce "online biographies." (Autenrieth 2018).

Because technology is widely available and the Internet is easy accessible, more than 81 percent of children worldwide have an online presence before the age of two. This digital footprint may begin before birth for some thrilled parents who post prenatal sonograms, or it may begin later with photos of a toddler's "firsts" or even whole accounts

on various social networking sites that capture the sweet nuances of a child's development (Brosch 2018).

The risk associated with this more advanced method of documenting the child development is that now it has a bigger audience than ever before, complemented with the potential for it to go viral (whether intentionally or not). In addition, parents frequently post information about their children online that might be harmful, like their full name, date of birth, or photos that might be humiliating to them. It should be clear parents leave a digital trail of material about their children online, which may have unintended repercussions both now and in the future. According to these, Eric Schmidt thinks every young person will one day be able to change their name to renounce humiliating digital pasts, since, nobody knows how nowadays information will be utilized to mold children's online experience (Holman / Jenkins 2010).

Also, there are many other grave risks. Due to harassing and humiliating children to increase internet views, parents have lost custody; YouTube routinely removes child-focused videos out of concern for their exploitation; public information on children's habits and whereabouts exposes them to pedophiles, child abductors and other criminals who target this vulnerable group (Ranzini, Newlands / Lutz 2020).

The conflict of a parent's right to share online with a child's right to privacy is still unsolved. Unfortunately, laws do nothing to shield children from oversharing by parents, even there are laws in existence that safeguard an individual's privacy in some situations. In fact, the child's right to privacy only shields them from strangers, but in practice, it should also protect them from any harm that parents may do by sharing overmuch personal information. Parents sometimes fail to realize they merely have the legal authority to act in the child's best interests and are not the actual data owners of their child.

Data Collection Practices of Mobile Applications

It has been found that mobile applications (apps) can gather digital identifiers and send them to third-party companies.

Tens of thousands of the millions of programs (apps) available on the Google Play and Apple App Stores are child-targeted games or educational apps (Zhao, at al. 2020). Children use these applications on a regular basis, whether they are playing video games, messaging friends, exploring social media, or watching movies. Ad technology is gathering

millions of pieces of personal data on their activity when they interact with these applications.

"Super Awesome Research" shows that "by the time a child is 13, over 72 million pieces of personal data will have been captured about them" (Mccann 2021). While children are playing it, Subway Surfer, Candy Crush Saga, Angry Birds, and even educational technology apps designed to teach children how to paint or help them with their schoolwork all spy on them (Pixalate 2022). These applications capture children's general geolocations and other personally identifiable data, such as their app usage patterns and past purchases, and sell it to businesses that track user interests and forecast what they might like to buy.

Digital privacy laws like COPPA (in the US) and GDPR (in Europe) have been enacted to make this illegal, but this type of data-harvesting technology continues being the fundamental engine of the Internet. COPPA's privacy protections only apply if it is known that a user is 13 years-old or younger. First, 13 is a completely arbitrary age for on-line users, and there's no good reason why you don't deserve privacy anymore when you are older. Second, no matter how old kids are, companies just have to get parental consent, then they can do nearly whatever they want with the data (COPPA 1998).

Article 8 of the GDPR effectively has the same requirements: "apps need verifiable parental consent before they can collect (but not process) data from children." GDPR protects more children. It applies to children under 16 (but individual states may lower the age to 13 or in between). Privacy Policy clauses are required too. They need to be written in language that children can understand, and they should outline clearly the opt-ins and opt-outs, as well as a description of parental rights. One step forward are GDPR's data minimization principles and they are clear that applications shouldn't gather data they don't need especially from children — and they should be clear about the data they do have, what they do with and how they delete it (European Union 2018).

But ultimately, it is up to the parents. They should examine the privacy rules of apps to check if they claim to be for adults only or if they share data with third parties. Therefore, unless we relieve busy parents of this responsibility, children's privacy is under risk every day.

CONCLUSION

Based on the above, it can be concluded that children's rights, especially children's privacy, are regulated by a large number of international regulations. At the European level, the right to privacy and the right to data protection are ensured both within the Council of Europe and within the European Union. The relevant law in the United States is the Children's Online Privacy Protection Act, which is enforced by the Federal Trade Commission. The most common violation of children's data and privacy was found to be online sharing, as well as the data collection practices of mobile applications. Of course, these are only some of the most common forms of abuse of children's data in cyberspace, but there are other forms that will appear at some point, given the rapid development of information and communication technologies.

Bearing in mind the above, it is necessary to take appropriate measures in order to more effectively protect children on the Internet and their personal data. In this regard, adequate steps should first be taken to educate children about cyber security and cyber threats. This should first of all refer to the use of social networks, measures to protect against fraud on the Internet, securing financial data, measures to protect computers from viruses and other malicious software. Secondly, it would be of great importance to use some parental control software, in order to gain control over the child's activities on the Internet, especially in terms of which websites are visited, the time spent on them, as well as insight into potentially malicious websites. Thirdly, the installation of adequate anti-virus programs in the devices used by children, as well as their regular updating, is of great importance. This applies not only to antivirus programs, but also to the Windows operating system and other accompanying software that children may use. Fourth, it is necessary to take appropriate steps in order to ensure the security of the home Internet network, as well as to educate children regarding access to public Wi-Fi networks. Finally, one of the main steps in protecting children in cyberspace and their personal data should be to create and nurture healthy virtual habits and cyber security awareness.

REFERENCES

Autenrieth, Ulla. 2018. "Family photography in a networked age: Anti-sharenting as a reaction to risk assessment and behaviour adaption." In *Digital Parenting: The Challenges for Families in the Digital Age*, by Giovanna Mascheroni, Christina Ponte and Ana Jorge, 219-231. Gothenburg: University of Gothenburg.

Barnes, Susan. 2006. "A privacy paradox: Social networking in the United States ." *First Monday* 11 (9). Accessed July 17, 2022. doi:https://doi.org/10.5210/fm.v11i9.1394.

Boban, Marija. 2012. "The right to privacy and the right to access information in the modern information society." *Collected papers of the Law Faculty of the University of Split* 49: 581-582.

Bošković, Milo. 2017. *Leksikon bezbednosti.* Novi Sad: Službeni glasnik.

Brosch, Ana. 2018. "Sharenting – Why Do Parents Violate Their Children's Privacy?" *The New Educational Review* 54: 75-85. Accessed March 11, 2023. doi: https://doi.org/10.15804/tner.2018.54.4.06.

Caglar, Cansu. 2021. "Children's Right to Privacy and Data Protection. Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?" *European Journal of Law and Technology* 12 (2). Accessed March 01, 2023. https://ejlt.org/index.php/ejlt/article/view/828.

Case of K.U. v. Finland. 2009. 2872/02 (ECHR, March 02). Accessed March 02, 2023. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-89964%22]}.

Case of Liberty and Others v. the United Kingdom. 2008. 58243/00 (European Court of Human Rights, July 01). Accessed March 06, 2022. https://data.guardint.org/en/entity/fmhlxe4x91l?page=1.

2000. *Charter of Fundamental Rights of the European Union*. December 18. Accessed March 10, 2023. https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Cho, Hichang, Rivera Rivera-Sanchez, and Lim Sun Sun. 2009. "A Multinational Study on Online Privacy: Global Concern and Local Responses." *New Media & Society* 11: 395-416.

Committee of Ministers. 2014. " Recommendation of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies)."

Council of Europe Committee of Ministers . April 16. Accessed March 05, 2023. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5b31.

—. 2008. "Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet." *Council of Europe Committee of Ministers*. February 20. Accessed March 05, 2023. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3d2d.

COPPA. 1998. *Children's Online Privacy Protection Act of 1998*. Accessed March 15, 2023. http://euro.ecom.cmu.edu/program/law/08-732/Regulatory/coppa.pdf.

Council of Europe. 2018. July 04. Accessed March 02, 2023. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808b79f7.

—. 2016. "Council of Europe." *Council of Europe Strategy for the Rights of the Child (2016-2021).* Accessed March 05, 2023. file:///D:/DOWNLOADS/017916GBR_StrategyChildren2016_2021.pdf.

—. n.d. "Council of Europe." *Modernisation of Convention 108*. Accessed March 08, 2023. https://www.coe.int/en/web/data-protection/convention108/modernised#.

Diggelmann, Oliver, and Maria Nicole Cleis. 2014. "How the Right to Privacy Became a Human Right." *Human Rights Law Review* 14 (3): 441. Accessed July 16, 2022. doi:10.1093/hrlr/ngu014.

Dimitrijević, Predrag. 2014. *Pravo informacione tehnologije*. Niš: Pravni fakultet u Nišu.

Autor. 2022.

Autor. 2022.

Autor. 2018.

European Union. 2018. *GDPR*. April 27. Accessed March 10, 2023. https://gdpr-info.eu/.

Garfinkel, Simson. 2000. *Database Nation : The Death of Privacy in the 21st Century* . Edited by Deborah Russel. Beijing: O'Reilly & Associates, Inc., 101 Morris Street, Sebastopol, CA 95472. http://index-of.co.uk/Misc/O%27Reilly%20Database%20Nation%20The%20Death%20of%20Privacy%20in%20the%2021st%20Century.pdf.

Gesley, Jenny. 2021. *Children's Online Privacy and Data Protection in Selected European Countries*. Library of Congress, 6-11. Accessed

March 10, 2023. https://tile.loc.gov/storage-services/service/ll/llglrd/2021680641/2021680641.pdf.

Holman, W., and Jr. Jenkins. 2010. *Google and the Search for the Future*. August 14. Accessed March 12, 2023. https://www.wsj.com/articles/SB10001424052748704901104575423294099527212.

Hsu, Hua. 2019. *The New Yorker*. September 11. Accessed March 10, 2023. https://www.newyorker.com/culture/cultural-comment/instagram-facebook-and-the-perils-of-sharenting.

Jovanović, Svetlana. 2014. *Privatnost i zaštita podataka na internetu*. Beograd, Srbija: Министарство унутрашњих послова Републике Србије.

Krasznay, Csaba, Judit Racz-Nagy, and Laszlo Dora . 2020. "Privacy Challenges in Children's Online Presence – From the Developers' Perspective." *Central and Eastern European eDem and eGov Days 2020*. Budapest. 149-158. Accessed March 10, 2023. https://ibn.idsi.md/vizualizare_articol/106820.

Krotz, Friedrich, and Andreas Hepp. 2011. "A concretization of mediatization: How 'mediatization works' and why mediatized worlds are a helpful concept for empirical mediatization research." *Empedocles European Journal for the Philosophy of Communication* 3 (2): 137-152. Accessed March 05, 2023. doi:10.1386/ejpc.3.2.137_1.

Kurland, Philip. 1976. "The Private." *University of Chicago Magazine* (The University of Chicago) 69 (1): 8.

Mascheroni, Giovanna . 2018. "Datafied childhoods: Contextualising datafication in everyday life." *Current Sociology* 68 (6): 798-813. doi:10.1177/0011392118807534.

Mccann, Duncan. 2021. *The billion-dollar business of surveillance advertising to kids*. May. Accessed March 10, 2023. https://neweconomics.org/uploads/files/i-Spy__NEF.pdf.

Mikulić v. Croatia Judgment. 2002. 53176/99 (European Court of Human Rights, February 7). Accessed March 06, 2022. http://www.aimjf.org/storage/www.aimjf.org/Jurisprudence_CEDU/CASE_OF_MIKULIC_v._CROATIA.pdf.

Milkaite , Ingrida, and Eva Lievens. 2019. "Children's Rights to Privacy and Data Protecton Aroundthe World: Challenges in the Digital Realm." *European Journal of Law and Technology* 10 (1). https://ejlt.org/index.php/ejlt/article/view/674/913.

Office of the High Commissioner for Human Rights. 1988. *CCPR General Comment No. 16: Article 17 (Right to Privacy) The*

Right to Respect of Privacy, Family, Home and Correspondence, and. New York, April 08. Accessed March 06, 2022. file:///D:/DOWNLOADS/453883f922.pdf.

Pixalate. 2022. *Mobille apps: Google v. Apple COPPA Scorecard (Children's Privacy).* Accessed March 12, 2022. https://www.pixalate.com/hubfs/Reports_and_Documents/Mobile%20Reports/2022/App%20Reports/Active%20Apps/Child-Directed%20Apps/Q1%202022%20-%20Apple%20vs.%20Google%20COPPA%20Scorecard%20Report%20-%20Pixalate.pdf.

Pretty v. United Kingdom Judgment. 2002. 2346/02 (European Court of Human Rights, April 29). Accessed March 06, 2022. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-60448%22]}.

Ranzini, Giulia, Gemma Newlands, and Christoph Lutz. 2020. "Sharenting, Peer Influence, and Privacy Concerns: A Study on the Instagram-Sharing Behaviors of Parents in the United Kingdom." *Social Media + Society.* Accessed March 12, 2023. doi:https://doi.org/10.1177/2056305120978337.

Sarat, Ostin. 2015. *A World without Privacy (What Law can and should Do?).* Cambridge: Cambirdge University Press.

Shah, Mahmood. 2013. "Online Social Networks: Privacy Threats and Defenses." In *Security and Privacy Preserving in Social Networks*, by Richard Chbeir and Bechara Al Bouna, 47-71. Vienna: Springer. doi:https://doi.org/10.1007/978-3-7091-0894-9.

Sinđelić, Žarko. 2012. *Pravo na privatnost-krivičnopravni, krivičnoprocesni i kriminalistički aspekti (Doctoral dissertation), p. 9.* Belgrade, Serbia. http://doiserbia.nb.rs/phd/fulltext/BG20120704SINDJELIC.pdf.

Štareikė, Eglė. 2022. "Features of the Legal Regulation Ensuring the Right of Minors to Private Life and the Protection of Personal Data." *Research Journal Public Security and Public Order* 30: 171-185.

UNCRC. 2021. "General comment No. 25 (2021) on children's rights in relation to the digital environment." *United Nations.* March 02. Accessed March 01, 2023. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

UNICEF. 2019. *Growing up in the connected world.* Accessed March 05, 2023. https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf.

United Nations. 1989. "Convention on the Rights of the Child text ." *Unicef* . Accessed March 01, 2023. https://www.unicef.org/child-rights-convention/convention-text.

United Nations General Assembly. 2013. *The right to privacy in the digital age.* New York, November 20. Accessed March 06, 2022. file:///D:/DOWNLOADS/A_C-3_68_L-45_Rev-1-EN.pdf.

United Nations General Assembly. 2014. *The Right to privacy in the Digital Age.* New York, June 30. Accessed March 19, 2022. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/088/54/PDF/G1408854.pdf?OpenElement.

United Nations General Assembly. 2015. *The right to privacy in the digital age: resolution.* United Nations. Accessed December 29, 2020. file:///C:/Users/S&B/AppData/Local/Temp/A_RES_69_166-EN.pdf.

United Nations. 2018. "UNESCO ." *UNESCO welcomes new UNHRC Resolution highlighting online freedom of expression and noting UNESCO Internet Universality Indicator Framework.* July 09. Accessed March 01, 2023. https://www.unesco.org/en/articles/unesco-welcomes-new-unhrc-resolution-highlighting-online-freedom-expression-and-noting-unesco.

Verdoodt, Valerie, Damian Clifford, and Eva Lievens. 2016. "Toying with children's emotions, the new game in town? The legality of advergames in the EU." *Computer Law & Security Review* 32 (4): 599-614. Accessed March 10, 2023. https://www.sciencedirect.com/science/article/abs/pii/S0267364916300851.

Warren, Samuel, and Louis Brandais. 1890. "The Right to Privacy." *Harvard Law Review.*

Zhao, Fangwei , Serge Egelman, Heidi Weeks, Niko Kaciroti, Alison Miller , and Jenny Radesky. 2020. "Data Collection Practices of Mobile Applications Played by Preschool-Aged Children ." *JAMA Pediatrics* 174 (12). Accessed March 12, 2023. doi:10.1001/jamapediatrics.2020.3345.

Синиша С. Домазет
Факултет за студије безбедности, Универзитет Едуконс, Сремска Каменица

Ивона Шушак-Лозановска
Правни факултет, Универзитет „Св. Климент Охридски“, Битољ

ДЕЧЈИ ПОДАЦИ И ОНЛАЈН ПРИВАТНОСТ – ОДРАСТАЊЕ У ДИГИТАЛНОМ ДОБУ

Сажетак

У дигиталној ери постоји безброј безбедносних проблема са којима се малолетници суочавају, али заштита приватности и података један је од главних изазова које законодавци треба да реше. Истраживања су показала да су права детета, посебно приватност деце, регулисана великим бројем међународних прописа. На европском нивоу, право на приватност и право на заштиту података обезбеђени су како у оквиру Савета Европе, тако и у оквиру Европске уније. Релевантни закон у Сједињеним Државама је Закон о заштити приватности деце на мрежи, који спроводи Федерална комисија за трговину. Утврђено је да је најчешће кршење приватности деце онлајн дељење, као и пракса прикупљања података мобилних апликација. Приватност деце на интернету може се побољшати бољом комуникацијом родитеља и деце у вези са коришћењем интернета, едукацијом деце о сајбер безбедности и онлајн претњама, коришћењем софтвера за родитељску контролу, инсталирањем антивирусних програма на уређаје које деца користе и слично.

Кључне речи: право, безбедност, сајбер простор, деца, приватност