DOMINIKA SKOCZYLAS

Administrative and Criminal Law Aspects of the Protection of Minors in Cyberspace: Selected Issues

Administracyjne i karnoprawne aspekty ochrony małoletnich w cyberprzestrzeni – wybrane zagadnienia

Abstract

The positive aspects of the use of electronic means of communication in administration, public and private services, on the one hand, and the potential threats to cybersecurity, on the other hand, lead to the assumption that the development of a specific digital security strategy is as necessary as the efficiency and effectiveness of e-actions. First of all, an important element of protection is to ensure the safe use of the Internet by minors. The aim of the article is to characterize the type of dangers that minors are exposed to when using the network. Administrative and penal measures that allow for the effective protection of minors in cyberspace are presented. The paper provides answers to the questions which aspects should be given special attention in the case of protection of children against electronic threats, in the context of personal data security and protection against e-pedophilia. The conducted research will allow to verify the research hypothesis, according to which the protection of underage Internet users cannot be limited only to parental control of content processed by minors on the Internet, but should be subject to special protection of the Polish legislator, public authorities and qualified institutions.

KEYWORDS: cyberthreats, e-personal data, e-pedophilia, minors, protection of minors

SŁOWA KLUCZOWE: cyberzagrożenia, e-dane osobowe, e-pedofilia, małoletni, ochrona małoletnich

DOMINIKA SKOCZYLAS – PhD in law, University of Szczecin,
ORCID – 0000-0003-1231-8078, e-mail: dominika.skoczylas@usz.edu.pl

HTTPS://DOI.ORG/10.36128/PRIW.VI52.607

1 Application of information and communication technologies – introduction

Information and Communication Technologies (ICT) and information infrastructure enable the exchange of information and the provision of services[1]. Electronic communication means are understood as technical solutions, including teleinformation devices and cooperating programming tools which enable an individual distance communication with the use of data transmission between teleinformation systems, in particular electronic mail[2]. As Aleksandra Monarcha-Matlak points out: „Through the use of information and communication technologies information and communication technologies, actions to develop society and the economy are possible"[3].

For citizens, an undeniable advantage of informatization is increased transparency, thanks to which public information is accessible to all on equal terms. The universality of the right to information is enshrined in the Constitution of the Republic of Poland of April 2, 1997[4]. Accessing and reading e-information or processing thereof depends on the preferences of individual network users, their actual and legal interests, the need to obtain specific information. The Internet initiated the „era of transparency of public information"[5], which in the traditional model of administration was reserved for public administration bodies and qualified institutions.

In the context of the information society founded on information, knowledge and skills, its main drivers being the development of electronic communications means, e-services and information technologies, establishing a legal framework for the protection of all Internet users, and in particular those who are the most vulnerable to cybercrime, is essential. Regrettably, electronic communication means can be used to perpetuate criminal acts,

1 Grażyna Szpor, *Jawność i jej ograniczenia. Tom. I: Idee i pojęcia* (Warszawa: C.H. Beck, 2016), 119.

2 Art. 2(5) of the Act of 18 July 2002 on providing services by electronic means (Journal of Laws 2020, item 344).

3 Aleksandra Monarcha-Matlak, „Usługa rejestrowanego doręczenia elektronicznego" *TEKA Komisji Prawniczej PAN Oddział w Lublinie*, No. 1 (2020): 297. https://doi.org/10.32084/tekapr.2020.13.1-22.

4 Journal of Laws No 78, item 483, as amended, further: RP Constitution.

5 Grzegorz Sibiga, „Jawność – tajność. Dokąd zmierzają relacje obywatela z władzą" *Monitor Prawniczy*, No. 2 (2019): 105-106. https://doi.org/10.32027/MOP.19.2.9.

acts detrimental to the society, and they can become an element of manipulation, intimidation, and create negative behavior patterns[6]. The youngest Internet users are the most vulnerable to the dangers of the Internet, and suffer the most from its effects. With regard to the subject of research, the key issue is to identify specific regulations of administrative and criminal law that ensure the protection of privacy, protection of children's personal data and protection from online pedophilia. Recently, „the number and type of threats in the cyberspace sphere implies the need to protect it"[7].

Minors, like adults, treat the Internet as a source of information, entertainment, and a means of interpersonal communication. However, minors are in many ways more vulnerable as Internet users. Because of little web skills or the naïve trust in other Internet users, minors may, unknowingly, give access to their personal data or be targeted by cybercriminals. Weighing the positive and negative aspects of ICT, the legislator's objective is to develop a strategy to ensure the safe use of the Internet by minors. Since, as network users, their personal data are continuously processed „[...] often without the interference of a data administrator, by unknown entities, for many purposes, with the use of varied means"[8], thus cybercriminals can easily gain access to certain kinds of personal data.

The aim of the paper is to specify the types of e-threats to which underage Internet users are particularly exposed. The author will point out administrative and penal measures, which allow for an effective protection of minors in cyberspace. The provisions of international law with regard to the so-called principle of the best interests of the child will be considered/analyzed. This principle forms the basis for the consideration of the protection of minors in cyberspace. The conducted research will allow to verify the research hypothesis, which claims that the protection of underage Internet users cannot be limited only to parental control of the content processed by minors on the Internet but should be subject to special protection of the Polish legislator, public authorities and qualified institutions.

---

6 Waldemar Krztoń, „XXI wiek – wiekiem społeczeństwa informacyjnego" *Modern Management Review*, No. 22 (2015): 108-109.

7 Dominika Skoczylas, „The Act on the National Cybersecurity System and Other Legal Regulations in the Context of Ensuring State Cybersecurity. Selected Issues" *Roczniki Nauk Prawnych*, No. 2 (2020): 103. https://doi.org/10.18290/rnp20302-7.

8 Michał Czerniawski, „Prawnie uzasadnione interesy jako podstawa przetwarzania danych online" *Prawo Mediów Elektronicznych*, No. 3 (2018): 33-34.

It seems that special attention should be paid to two fundamental problems related to the safety of minors in cyberspace: the security of personal data and protection against online pedophilia. In extraordinary circumstances, when the child's welfare is threatened, all necessary legal measures should be taken, including preventive and follow-up measures, to ensure effective protection against cyberdangers. Parental control is fundamental in the use of technology, but when a cyberdanger develops into a cybercrime, the law should intervene and relevant provisions of administrative and criminal law should be applied.

The paper attempts to answer the question of which aspects of the protection of minors from the dangers of the Internet should be given special attention in the context of personal data security and protection from e-pedophilia. The first part of the paper covers the use of electronic communication means in information society, including minors, with particular emphasis on the so-called child welfare principles. The second part presents the administrative and criminal law aspects of the safety of minors online. In order to verify the research hypothesis, regulations concerning the security of personal data, the criminal law protection of minors in cyberspace and aspects of parental control were analyzed. The role of the Ombudsman for Children's Rights was outlined, and further, based on the acts of international law, the concept of child welfare was examined.

The formal and legal method and the comparative method were applied in the study. Apart from theoretical considerations, an equally important part of this study focuses on the aspects of parental control. In addition, the results of research on the types of dangers to which minors are exposed in cyberspace are presented. The research methods include the analysis of legal acts using the literature on the subject.

2 The use of electronic means of communication in the context of the information society. Child welfare and cyberthreats

Digital media and the Internet bring so many benefits that it has become a specific public good, which the information society identifies with basic human and civil rights. For today's high-tech society, computerization and

digitization allow almost unlimited consumption, sharing and processing of information, in contrast to the so-called „traditional media"[9]. The Internet as a channel of communication, and in particular the content that appears on websites, including network websites, should be subject to close scrutiny by the authorities. The protection of human rights is guaranteed by the state and is the responsibility of certain public administrative bodies, which are obliged to ensure the safe use of the Internet, while ensuring that freedom of expression, freedom of transactions and freedom of services are respected[10]. Special protection should be provided to minors, unaware of potential online dangers, for whom the online reality is often as real as the offline reality of the world, hence the term „virtual reality" is so commonly used these days.

Minors, that is children and youths, constitute a special category of the information society. The way minors use the Internet is conditioned not only by the role of information and technology in today's world, but also by the social aspect of the digital media and the social needs they have created, such as the need to keep up with the latest news and trends, and to stay in touch with their peers. As it is the case with adult Internet users, minors are interested in specific sectors of the ICT: education, R&D, entertainment, interpersonal communication and online services[11]. Minors' activity online depends on the age group they represent, and so, it ranges from computer games, learning tools, social media, online purchases, offering services and making transactions. Unfortunately, minors are particularly vulnerable to the exploitation of online predators and are often targeted by cybercriminals. This happens because, firstly, minors are not yet able to foresee the consequences of their online activities, secondly, at this age they are predisposed to trust other Internet users, and thirdly, they are less critical than adults, more susceptible to manipulation and addiction, and tend to treat virtual reality as reality per se.

---

9 Christian Fuchs, „Information Technology and Sustainability in the Information Society" *International Journal of Communication*, No. 11 (2017): 2433.

10 Andrzej Nałęcz, „Bardziej człowiecze podejście – prawa człowieka w prawie gospodarczym na przykładzie unormowania dostępu do Internetu", [in:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. Barbara Jaworska-Dębska, Przemysław Kledzik, Janusz Sługocki (Warszawa: Wolters Kluwer, 2020), 397.

11 Peter Sasvari, „The Role of Technology and Innovation in the Framework of the Information Society" *International Journal of Advanced Research in Artificial Intelligence*, No. 2 (2012): 33-34. https://doi.org/10.14569/IJARAI.2012.010206.

A large Polish NGO, the Empowering Children Foundation, and a public institute, NASK – Research and Academic Computer Network which operates under the Safer Internet Programme, promote the awareness of potential Internet risks for minors, including issues such as cyberbullying, sexting, grooming, cyberdating, sextortion and harmful content. Institutions and NGOs encourage parents to implement parental control over Internet content. This control takes many possible forms, from open communication with the child about the websites he/she visits, online forums and social media platforms where he/she is an active user, to the use of specific parental control tools that help monitor the child's activities on the Internet, such as Norton Family, Kaspersky SafeKids, Mobikid or Kids Place (available for Android). Research conducted by NASK in 2016 shows that as much as 93,4% of kids browse the net from home every day. Although it is not a disturbing fact in itself, considered the digital age environment, what raises concerns is that 32% of Polish minors aged 7-18 has been exposed to online erotica and pornography (the Empowering Children Foundation, 2018 research), which is indeed a serious threat[12].

De facto, cyberattacks are facilitated by such ICT features as: „multimediality and individualization of message, increased interactivity, multifunctionality, accessibility and also the social aspect of social media"[13]. When it comes to the youngest Internet users, the highest risk is connected with social media. The publication of photos and information without the consent of the owner, the coercion of children to behave in a certain, involuntary way with the use of their personal data, Internet fraud and e-pedophilia are the most common Internet dangers that minors are exposed to.

The 2019 report on child online safety created by the UN Broadband Commission for Sustainable Development, examines the causes and effects of Internet dangers and recommends actions that should be pursued to ensure children's online safety. What is truly alarming about the report's findings is that only 72% of countries have functional cybercrime legislation. Moreover, even within these countries, there is often lack of consistent legal and operational definitions of what is an „online threat", and lack of coordinated action between different agencies. Because of this, cybercriminals

12 Dziecko w sieci. http://www.dzieckowsieci.pl/ [dostęp: 28.12.2022].

13 Barbara Antczak, „Social Media as a Field for a Company's Brand Development" *Teka Commission of Legal Sciences. Polish Academy of Sciences, Branch in Lublin*, No. 2 (2019): 10-11. https://doi.org/10.32084/tekapr.2019.12.2-1.

can act with impunity worldwide[14]. In this regard, the Office of Electronic Communications (OEC) has a special role in Poland, which is responsible for the overall supervision of the Internet in Poland, including tasks such as the assessment of online risks for minors. The report highlights the crucial role of education of teachers, parents, caregivers, and finally children, as means to reduce online harm[15].

A consumer study of children and parents conducted in 2020 by OCE emphasizes that parental control is essential to ensuring that the Internet is used responsibly and safely by children. The study reveals that about 66% of Polish parents applies some means of the so-called parental control. Usually, this control is about setting Internet rules, deciding together with children what they will be, and open conversations about online experiences[16]. Parental control is the key element in preventing online harm. Parents should take the responsibility for educating their children how to use the Internet safely and responsibly and teach them the basics of netiquette. Lack of parental control makes it easy for cybercriminals to penetrate into the online environment of a minor. Intensive online interaction may be used by cybercriminals to convey harmful content, e.g. pornography, to promote cyberviolence or e-pedophilia. As possible remedy is to use blocking technologies – apps – to block problematic websites or to limit child's Internet time. Nonetheless, it seems that parents' efforts should be supported by school teachers. In the words of Katarzyna Derlatka: „it is necessary to introduce dedicated classes on online safety and threats in our curricula"[17]. Such joined educational efforts, involving parents, caregivers and teachers, should bring positive results and protect children from online harm.

Cyberattacks targeted at minors come in various forms: exposure to pornographic content, child sexual abuse material, content promoting hate and violence, offering abusive services, grooming, sexting, pressure

14 Bezpieczeństwo dzieci online – raport Komisji Szerokopasmowej ONZ, 41. https://www.uke.gov.pl/akt/bezpieczenstwo-dzieci-online-raport-komisji-szerokopasmowej-onz,248.html [dostęp: 28.12.2022].

15 Ibidem, 66. https://www.uke.gov.pl/akt/bezpieczenstwo-dzieci-online-raport-komisji-szerokopasmowej-onz,248.html [dostęp: 28.12.2022].

16 Badanie konsumenckie dzieci i rodziców oraz nauczycieli 2020. https://www.uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html [dostęp: 28.12.2022].

17 Katarzyna Derlatka, „Cyberzagrożenia w edukacji dla bezpieczeństwa i świadomość uczniów w obszarze bezpieczeństwa Internetu" *Interdyscyplinarne Studia Społeczne*, No.1 (2017): 36.

for sex, interception of financial transactions, disclosure of financial or confidential data[18]. Parents, who exercise control over what their children do and see online, play the key role in keeping children safe online.

The ever-growing amount of „screen time" hat minors spend on electronic communication and the complex nature of cyberthreats is an issue of concern around the world. Many actors in the field of child online safety space around the world are committed to creating an online world that is safe for children. It is a mistake to assume that the lack of immediate action and distance communication is something harmless. It must also be remembered that promoting children's rights is as important as important as raising awareness of child online safety. Considering how broad the issue of online child protection is, it is worth to analyze the measures adopted by the Polish legislator with regard to two important aspects: protection of minors' personal data and protection against cybercrime understood as the propagation of pornography and e-pedophilia.

When it comes to children's rights' legislation, standards for the protection of children's rights are set by the Convention on the Rights of the Child [CRC] of November 20, 1989[19]. The Convention does not refer directly to children's online safety, but it does contain legal provisions that define the measures that should be taken to ensure safety in the broad sense. The ones that are relevant to the topic discussed herein are: ensuring that in all actions taken by courts of law, administrative authorities or legislative bodies and public or private social welfare institutions, the best interests of the child will be a primary concern (Art. 3 CRC), ensuring that the child will have the right to freedom of expression through any form or media of choice (Art. 13 CRC), recognizing the importance of the mass media, including its responsibility for providing guidelines to protect the child from information and material injurious to the child's wellbeing (Art. 17 CRC), the obligation to take legislative, social and educational measures to protect the child from all forms of physical or mental violence, child abuse and neglect, and any other forms of criminal act (Art. 19 CRC).

The whole Convention emphasizes the so-called „child welfare". This concept is also present in Polish law, i.a. in the Constitution of the Republic

18 Agnieszka Filipek, „Dziecko w kontekście zagrożeń Internetu", [in:] *Wielowymiarowość przestrzeni życia współczesnego dziecka*, red. Jadwiga Izdebska, Joanna Szymanowska (Białystok: Trans Humana Wydawnictwo Uniwersyteckie, 2009), 376.

19 Journal of Laws 1991 No 120, item 526, hereinafter: CRC.

of Poland, and the Family and Guardianship Code. An attempt at interpretation makes one think that is the the so-called general clause, a legislative construct that requires concretizing in the context of individual cases of child abuse. Child welfare is paramount, and it is linked to the „child's best interest, spirituals values, material values and representation in the law", which should be treated as a guideline on how to proceed[20]. This rule should be applied in administrative and criminal law protection of children against cyberthreats. The system of human rights law with regard to human dignity and right to privacy, as well as the protection of these rights, points to the special nature of human rights, including child's rights, reflected in the fact that „dignity as a (human, personal) value is universal and therefore an intrinsic part of every human being"[21]. In the context discussed, it is positive that respect for the child as Internet user and creating legal safeguards against online harm are encompassed by the child welfare principle.

3 Security of online personal data and protection of minors from e-pedophilia – administrative and criminal law analysis

The question is – from what types of online harm should minors be particularly protected by the Polish legislator? What seems to be the core areas that need a legal framework are the protection of information online, including personal information, and protection from cybercrime in form of child pornography and online sexual predators. In the cyberworld, minors are constantly being exposed to information, and when this information is credible and attractive, children are prone to trust online strangers and may

20 Patrycja Sołtysiak, „Zasada dobra dziecka", [in:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. Barbara Jaworska-Dębska, Przemysław Kledzik, Janusz Sługocki (Warszawa: Wolters Kluwer, 2020), 434-435.

21 Daria Bieńkowska, „Powszechna Deklaracja Praw Człowieka jako inspiracja dla współczesnych reżimów praw człowieka", [in:] *Prawa człowieka i ludzkie bezpieczeństwo. Osiągnięcia i wyzwania w 70. Rocznicę Ogłoszenia Powszechnej Deklaracji Praw Człowieka*, red. Daria Bieńkowska, Ryszard Kozłowski (Warszawa: C.H. Beck, 2019), 21-22.

be interested in the content presented by them. The right to the freedom of expression cannot breach other applicable legal norms[22], and thus it does not apply to actions that may harm (emotionally or physically) or abuse minors. In the Polish legal system, the basic principles of children's rights protection are laid down in Art. 72 of the RP Constitution.

Administrative regulations enforcing the protection of children's rights determine general goals dictated by the child's welfare principle and assign relevant legislative and executive tasks to public authorities and institutions. Regulation (EU) 2016/679 of the European Parliament and 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), referred to as the GDPR[23], provides administrative provisions that warrant a higher standard of children's online safety. Aside from provisions that regard every natural person, the GDPR addresses the issue of protection of children's data. As rightly noticed by Krzysztof Dzioba and Angelika Kosińska, with regard to children, the GDPR sets: „[...] much more restrictive standards than for adult persons. These standards will have to be met by, first and foremost, personal data administrators who offer information society services and process data on the basis of consent"[24]. The solutions for the safety of children in the online world are expressed in the preamble to the GDPR. Recital 38 of the GDPR provides that children, who are less aware of the risks, consequences and safeguards and their rights in relation to the processing of personal data, should merit specific protection which, in particular, should apply to the use of their personal data 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. In turn, Recital 58 focuses on the principle of transparency, emphasizing that where processing is addressed to a child, any information and communication should be in such a clear and plain language that the child can easily understand. Recital 75 addresses the issue of inappropriate processing of personal data, i.e. the risks to the rights and

22 Aleksandra Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem* (Warszawa: Wolters Kluwer, 2010), 48-49.

23 OJ L 119, 4.5.2016, p.1.

24 Krzysztof Dzioba, Angelika Kosińska, „Ochrona danych osobowych w szkole w związku z rozpoczęciem stosowania RODO oraz nowej ustawy o ochronie danych osobowych" *Informacja w Administracji Publicznej*, No. 4 (2017): 20.

freedoms of data subjects resulting in physical, material or non-material, in particular where personal data of children are processed.

A heightened awareness of potential online harms led the legislator to introduce the so-called „conditions applicable to child's consent in relation to information society services". Art. 8 of the GDPR provides that in relation to information society services offered directly to a child, the processing of a child's personal data shall be lawful where the child is at least 16 years old and gives his/her consent to data processing. Whereas, in case of children below 16 years of age, the processing shall be lawful only if the consent by the holder of parental responsibility over the child is given or authorized. In exceptional circumstances, member states may provide by law for a lower age, but not lower than below 13 years.

Another important aspect is the technology used by the administrator to verify whether the holders of parental responsibility have in fact given their consent to online data processing[25]. Online authentication and identification are quite a challenge for personal data administrators. It is not easy to verify the age of an Internet user and the credibility of the consent given by a parent or guardian. The administrator may be misled about the age of the minor on purpose. In the first place, the administrator is responsible for the processing of personal data, and in case of any doubts about the Internet user's age, he should prohibit the use of the user's data for marketing or profiling purposes[26].

The Charter of Fundamental Rights of the European Union (the Charter) incorporating basic human rights into the EU legislative process, safeguards children's rights on the Internet[27]. Art. 24 of the Charter safeguards the children's right to such protection and care as is necessary for their well-being and the right to the freedom of expression and provides that public authorities and private institutions shall take adequate actions to protect the children's best interests. In turn, Art. 7 lays down the universal principle which protects „electronic communication with a natural person,

25 Paweł Fajgielski, „Zgoda na przetwarzanie danych osobowych w przepisach ogólnego rozporządzenia o ochronie danych" *Informacja w Administracji Publicznej*, No. 4 (2016): 11-12.

26 Maciej Giermak, Małgorzata Sofronów, „Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego" *Monitor Prawniczy*, No. 2 (2017): 96-97.

27 OJ C 326, 26.10.2012, p. 391-407.

to be qualified as personal data"[28]. Hence, it can be said that the principle provides by Art. 7 of the Charter set a blueprint for privacy laws, including the protection of personal data collected in electronic databases. In fact, children's well-being and their protection from online harm is one of the core responsibilities of public authorities.

Before we delve into Polish legal framework for the protection of minors on the Internet, it is worth presenting the main provisions of the Council of Europe Convention on Cybercrime drafted in Budapest on 23 November 2001 (Budapest Convention)[29]. The Convention aims to address child Internet crime; i.a., it specifies types of cybercrime and imposes obligations to adopt such legislative and other measures as may be necessary for the offence to be established as cybercrime under domestic law. Offences related to child pornography (Art. 9 of the Budapest Convention) were considered among the most serious cybercrimes regarding children. The scope of the criminalization of child pornography is very broad as it encompasses for example, making available child pornography (images, films) or any realistic images depicting a minor engaged in sexually explicit conduct, or any conduct involving the production, offering, possession or distribution of child pornography through a computer system[30].

In the context of the protection of children's personal data, Art. 2 and 3 of the Budapest Convention deserve special attention. Both adults and minors are exposed to cybercriminals and their actions – from security breaches to identity theft. These are offences that are committed by infringing security measures with the intent to obtain computer data, or interception made by technical means, without right, of non-public transmissions of computer data to, from or within a computer system. The Budapest Convention provides that adequate legislative measures should be adopted as may be necessary to empower the state's competent authorities to order the following measures: expedited preservation of stored computer data (Art. 16 Budapest Convention), search and seizure of stored computer data (Art. 19 Budapest Convention), and interception of content data (Art. 21 Budapest Convention).

---

28 Xawery Konarski, „Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenia o ochronie danych osobowych (RODO)" *Monitor Prawniczy (supplement MoP)*, No. 20 (2017): 6.

29 Journal of Laws 2015, item 728, further: Budapest Convention.

30 Maciej Siwicki, „Przestępstwa związane z treścią informacji" *Edukacja Prawnicza*, No. 10 (2012): 26-27.

Based on the provisions of the Budapest Convention, the Polish legislator, in the Act of June 6, 1997 – Criminal Code[31], punishes crimes committed against minors who use the Internet. These include, i.a., the use of threats (Art. 190, 191 CC), persistent harassment (Art. 190a), displaying pornographic material (Art. 202), slander (art. 212), insult (Art. 216) and illegal access to information (Art. 267). Cybercrime takes many forms, from cyberbullying through cyberstalking to cyberharsassment. The common denominator here is the impact of such abusive conduct on the victim, namely the sense of helplessness, fear, rejection, or even an offence[32]. A good solution would be to adopt a criminal law framework and to create specific guidelines for the management of children's personal data online. Another danger to minors on the Internet is pornography and online pedophilia. Online sexual predators may:

- present or offer pornographic material, or distribute or propagate pornographic content in such a way that minors are exposed to it (Art. 200 CC),
- produce or preserve pornographic materials, by an information system or telecommunications network, to establish a connection with a minor with the intention of using deceit or unlawful threat, exploiting the child's inability to understand the situation, or through making unlawful threats in order to meet him/her or make offers of sexual intercourse, to have sexual intercourse, submit or perform another sexual act, or participate in the production or preservation of pornographic content (Art. 200a CC). The Criminal Code extends protection to minors under the age of 15.

The anonymity of cybercriminals, coupled with children's lack of awareness of online sexual threats and a contact facilitated by the networking era leads to the so-called online „grooming" of children. Finding perpetrators of such crimes requires law enforcement agencies to collect and evaluate physical evidence including: IP logs, records of IT applications used by the person accused of pedophilic acts, electronic correspondence, billing records. It must be noted that the said anonymity of Internet users is often

31 Journal of Laws 2024, item 17, 1228, as amended, further: CC.

32 Łukasz Wojtasik, „Cyberprzemoc", [in:] *Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów,* red. Agnieszka Wrzesień-Gandolfo (Warszawa: Polskie Centrum Programu Safer Internet Warszawa 2014), 16-18.

illusory as the Internet user can be identified by IP address or cookies[33]. Naturally, parents should warn children of online risks and sensitize them to suspicious behavior of other Internet users, but in case of conduct that shows features of a criminal offence, such as the distribution of child pornography or online pedophilia, criminal law protection is an indispensable condition both for preventive measures (before the criteria of a criminal offence are met) and for follow-up measures (finding and punishing the perpetrator).

According to the 2019 report on problematic use of the Internet by youths, presented by the Empowering Children Foundation, 54,4% of young people had contact with inappropriate online content. One in three was exposed to violence on the Internet, and one in four to content related to self-harm, pornographic content, offensive content, and content promoting discrimination[34]. The Act of 30 August 2019 on the State Commission for the examination of acts against sexual freedom and sexual integrity of minors below 15 years of age[35] emphasizes the urgent need to protect minors in cyberspace, in particular against sexually-abusive content and sexual grooming. The work of the Commission with regard to informative, preventive and educational activities (preparation and publication of relevant reports) aim at sexual abuse protection and prevention minors.

Finally, it is worth adding that the Constitution grants a special competence to the Ombudsman for Children's Rights who, in accordance with the Act on the Ombudsman for Children of 6 January 2000 (AOC)[36], shall protect children's rights enshrined in the Constitution of the Republic of Poland, the Convention on the Rights of the Child and other provisions of law, while respecting the responsibility, rights and obligations of parents (Art. 1 section 2 (AOC). The Ombudsman for Children safeguards and promotes the rights and freedoms of children in Poland. The Ombudsman takes action on its own initiative, according to the acts of law, to protect minors from violence, exploitation, demoralization, neglect and other forms of maltreatment. The child is perceived as a separate holder of rights

33 Arkadiusz Lach, „Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie" *Prokuratura i Prawo*, No. 10 (2005): 55-57.

34 Problematyczne używanie Internetu przez młodzież. Raport z badań, 6. https://fdds.pl/_Resources/Persistent/d/1/6/4/d164e2f03eba3e6195f1dae6da1934177afedfe0/Problematyczne-uzywanie-internetu-przez-mlodziez-Raport-z-badan.pdf [dostęp: 29.12.2022 r.].

35 Journal of Laws 2024, item 94.

36 Journal of Laws 2023, item 292, as amended, further: AOC.

and freedoms, including economic, social and cultural rights, deserving respect in all areas of life in which he/she exercises their rights. Moreover, as children are not mature emotionally and mentally, are dependent on adults and unable to protect themselves, they need support and legal protection from the state and public institutions, even more so when they become a victim of a crime[37]. The Ombudsman for Children can intervene in administrative, civil and criminal law proceedings (Art. 10 AOC).

4 Conclusions

From the above findings, it can be concluded that underage Internet users are particularly vulnerable to cybercrime. In the context of the rapid development of the information society, we must recognize that the increased use of ICT is accompanied by an increase in cybercrime. As the above analysis suggests, the most common types of cybercrime are: misuse personal data, cyberviolence e.g. cyberharassment, unlawful threats, distribution of pornography and online pedophilia. The length of this list raises many serious concerns. For minors, the Internet is a source of entertainment and knowledge, and not only a platform for networking and connecting, but a medium for mass social interaction. Therefore, lack of caution and IT skills on the one hand, combined with hacking and cyberscams on the other often lead to a massive disclosure of personal data.

In an exceptional situation where the child's well-being is at risk, all necessary legal measures should be taken to ensure effective protection from online harm. Parental control is crucial, but it cannot be limited to blocking access to certain websites or monitoring screen time. Parents need to talk openly about the positive and negative aspects of Internet use, guide their children in using the Internet safely, teach them netiquette and the basics of safe and appropriate communication with others so that they are able to recognize inappropriate and unwanted content. Lack of parental control makes children more vulnerable to online predators. Clearly, schools providing e-safety curriculum would be of great support to parents. On the other hand, when digital risk turns into cybercrime,

37 Agnieszka Krawczak-Chmielecka, „O rozwoju praw dziecka w Polsce i na świecie" *Dziecko Krzywdzone. Teoria, badania, praktyka*, No. 2 (2017):18-19.

public administrations and law enforcement agencies need to respond. However, the above analysis has proven the research hypothesis to be true: the protection of underage Internet users cannot be limited to parental control of online content, but should come under the special protection of the Polish legislator, public authorities and qualified institutions, which is indeed the case.

It is obvious that public administrations need to take into account that as technology advances, digital risks may become more complex, cybercriminals may become more aggressive and active, and the identification of predators may become more difficult. Therefore, not only the legal system, but also the IT systems of public institutions responsible for cybersafety and cybersecurity must adapt to the rapidly changing online environment. This is especially true for the implementation of the principle of the best interests of the child, the security of the child's personal data and the protection against online pedophilia and cyberviolence. As a result, the Polish legislator adopts special solutions that help to protect or minimize the negative effects of Internet crimes against children. The provisions of the GDPR, the Criminal Code and the mission of the Children's Ombudsman give importance to the fundamental principle of the best interests of the child, which is at the core of international legislation

In light of the above considerations, it can be concluded that the security of children's personal data, the protection of their privacy and their protection from cyberviolence require a thorough and detailed regulation of administrative and criminal law protection. This requirement is linked to the nature of the digital risks to which minors are exposed on the Internet. Undoubtedly, the GDPR's provisions on children's online safety have made a difference, in particular the prohibition on using children's personal data for marketing or profiling purposes, the requirement that messages be tailored to and understood by children, and the provisions on children's consent in the provision of information society services. The criminalization of Internet crimes against children also deserves recognition. Acknowledging the problems of personal data security on the Internet, such issues as cyberbullying and cyberstalking, allows the state to adopt a legal framework (criminal law) and develop special policies on children's personal data administration. It is essential for the legislator to pay attention to some specific aspects on children's online safety. Rapid development of ICT and social media creates a context – a new cyberworld – in which privacy laws must be tightens and sanctions against cybercriminals effective. In view of the type of digital services offered to

children, online safety-related education of children should be developed and collaboration with public and private entities, as well as service providers, strengthened. The legislator's role is also to promote parental control and school education regarding children's online safety.

In conclusion, the legislative measures adopted, together with wise and comprehensive parental control, should ensure better protection of children's welfare. Adults (parents, public and private entities, specialized institutions) are obliged by law to take care of children, to fulfill, protect and respect their rights, using administrative and penal measures, in particular in the present virtual world, in which many Internet risks to child safety are brought about by user anonymity and cannot be foreseen.

Bibliography

Antczak Barbara, „Social Media as a Field for a Company's Brand Development" *Teka Commission of Legal Sciences. Polish Academy of Sciences, Branch in Lublin*, No. 2 (2019): 5-19. https://doi.org/10.32084/tekapr.2019.12.2-1.

Badanie konsumenckie dzieci i rodziców oraz nauczycieli 2020. https://www.uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html.

Bezpieczeństwo dzieci online – raport Komisji Szerokopasmowej ONZ. https://www.uke.gov.pl/akt/bezpieczenstwo-dzieci-online-raport-komisji-szerokopasmowej-onz,248.html.

Bieńkowska Daria, „Powszechna Deklaracja Praw Człowieka jako inspiracja dla współczesnych reżimów praw człowieka". [in:] *Prawa człowieka i ludzkie bezpieczeństwo. Osiągnięcia i wyzwania w 70. Rocznicę Ogłoszenia Powszechnej Deklaracji Praw Człowieka*, red. Daria Bieńkowska, Ryszard Kozłowski. 13-23, Warszawa: C.H. Beck, 2019.

Czerniawski Michał, „Prawnie uzasadnione interesy jako podstawa przetwarzania danych online" *Prawo Mediów Elektronicznych*, No. 3 (2018): 33-37.

Derlatka Katarzyna, „Cyberzagrożenia w edukacji dla bezpieczeństwa i świadomość uczniów w obszarze bezpieczeństwa Internetu" *Interdyscyplinarne Studia Społeczne*, No. 1 (2017): 23-40.

Dziecko w sieci. http://www.dzieckowsieci.pl/.

Dzioba Krzysztof, Angelika Kosińska, „Ochrona danych osobowych w szkole w związku z rozpoczęciem stosowania RODO oraz nowej ustawy o ochronie danych osobowych" *Informacja w Administracji Publicznej*, No. 4 (2017): 20.

Fajgielski Paweł, „Zgoda na przetwarzanie danych osobowych w przepisach ogólnego rozporządzenia o ochronie danych" *Informacja w Administracji Publicznej*, No. 4 (2016): 9-12.

Filipek Agnieszka, „Dziecko w kontekście zagrożeń Internetu, [w:] *Wielowymiarowość przestrzeni życia współczesnego dziecka*, red. Jadwiga Izdebska, Joanna Szymanowska. 375-385. Białystok: Trans Humana Wydawnictwo Uniwersyteckie, 2009.

Fuchs Christian, „Information Technology and Sustainability in the Information Society". *International Journal of Communication*, No. 11 (2017): 2431-2461.

Giermak Maciej, Małgorzata Sofronów, „Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego" *Monitor Prawniczy*, No. 2 (2017): 93-97.

Konarski Xawery, „Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenia o ochronie danych osobowych (RODO)" *Monitor Prawniczy (supplement MoP)*, No. 20 (2017): 6-13.

Krawczak-Chmielecka Agnieszka, „O rozwoju praw dziecka w Polsce i na świecie" *Dziecko Krzywdzone. Teoria, badania, praktyka*, No. 2 (2017): 11-23.

Krztoń Waldemar, „XXI wiek – wiekiem społeczeństwa informacyjnego" *Modern Management Review*, No. 22 (2015): 101-112.

Lach Arkadiusz, „Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie" *Prokuratura i Prawo*, No. 10 (2005): 52-62.

Monarcha-Matlak Aleksandra, „Usługa rejestrowanego doręczenia elektronicznego" *TEKA Komisji Prawniczej PAN Oddział w Lublinie*, No. 1 (2020): 287-298. https://doi.org/10.32084/tekapr.2020.13.1-22.

Nałęcz Andrzej, „Bardziej człowiecze podejście – prawa człowieka w prawie gospodarczym na przykładzie unormowania dostępu do Internetu", [in:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. Barbara Jaworska-Dębska, Przemysław Kledzik, Janusz Sługocki. 388-398. Warszawa: Wolters Kluwer, 2020.

Problematyczne używanie Internetu przez młodzież. Raport z badań. https://fdds.pl/_Resources/Persistent/d/1/6/4/d164e2f03eba3e6195f1dae6da1934177afedfe0/Problematyczne-uzywanie-internetu-przez-mlodziez-Raport-z-badan.pdf.

Sasvari Peter, „The Role of Technology and Innovation in the Framework of the Information Society" *International Journal of Advanced Research in Artificial Intelligence*, No. 2 (2012): 31-38. https://doi.org/10.14569/IJARAI.2012.010206.

Sibiga Grzegorz, „Jawność – tajność. Dokąd zmierzają relacje obywatela z władzą" *Monitor Prawniczy*, No. 2 (2019):105-109. https://doi.org/10.32027/MOP.19.2.9.

Siwicki Maciej, „Przestępstwa związane z treścią informacji" *Edukacja Prawnicza*, No. 10 (2012): 25-29.

Skoczylas Dominika, „The Act on the National Cybersecurity System and Other Legal Regulations in the Context of Ensuring State Cybersecurity. Selected Issues" *Roczniki Nauk Prawnych*, No. 2 (2020): 93-113. https://doi.org/10.18290/rnp20302-7.

Sołtysiak Patrycja, „Zasada dobra dziecka", [in:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. Barbara Jaworska-Dębska, Przemysław Kledzik, Janusz Sługocki. 429-436. Warszawa: Wolters Kluwer, 2020.

Suchorzewska Aleksandra, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*. Warszawa: Wolters Kluwer, 2010.

Szpor Grażyna, *Jawność i jej ograniczenia. Tom. I: Idee i pojęcia.* Warszawa: C.H. Beck, 2016.

Wojtasik Łukasz, „Cyberprzemoc", [in:] *Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów*, red. Agnieszka Wrzesień-Gandolfo. 15-21. Warszawa: Polskie Centrum Programu Safer Internet Warszawa 2014.