| Chapter 9 |

Children in Digital Age – Polish Perspective

Agnieszka Gryszczyńska

ABSTRACT

Internet usage among children and young people offers both advantages and potential risks. These diverse risks have consequences across various areas of life – physical, psychological, and social – and, therefore, require differentiated regulatory, organisational, and educational responses. This chapter examines the regulations in Poland concerning the safeguarding of children in cyberspace. It investigates the principles of safeguarding children under civil, administrative, and criminal law. The study verifies the hypothesis of the completeness and consistency of measures to protect children from new threats arising from modern technologies and widespread Internet access. The legal framework for safeguarding children and the roles of relevant agencies are outlined. Special attention is given to the capabilities of the Ombudsman for Children, the Dyżurnet team operating within the Scientific and Academic Computer Network, and law enforcement bodies specialising in the combating of cybercrime, including child sexual abuse material. To improve the efficiency of combating cybercrime, including offences committed against children, specialised units in the police and prosecutors' offices have been established. In 2022, the police established the Central Bureau for Combating Cybercrime, while the National Public Prosecutor's Office created the Department for Cybercrime and Informatisation, as well as cybercrime units in selected circuit and regional prosecutors' offices. Amendments to the Sexual Offences Threat Act have also been introduced, providing a more comprehensive approach to child protection. It is only through the application of these regulations over time that their efficacy in enhancing children's online protection can be ascertained. To ensure an adequate level of protection for children's rights in cyberspace, specific regulations have been analysed regarding the development of digital competences in Poland, including the Digital Competence Development Programme. Importantly, only appropriate education and the development of digital competences, including incident response and corresponding attitudes, can ensure an adequate level of protection for children's rights in cyberspace.

KEYWORDS

legal child protection, cyberspace, cybercrime, child sexual abuse material, cyberstalking, FOMO, grooming

Agnieszka Gryszczyńska (2025) 'Children in Digital Age – Polish Perspective' in Halász, Cs. (ed.) *Children in Digital Age*. Miskolc–Budapest: Central European Academic Publishing, pp. 171–197. https://doi.org/10.71009/2025.csh.cida_9.

1. Introduction

Internet usage among children and young people offers both advantages and substantial risks. A wide range of risks, such as exposure to age-inappropriate content, child sexual abuse material, cyberbullying, and cybercrime, can have ramifications for physical, mental, and social well-being.

The Internet's availability, ease of use, and anonymity create an environment that can prompt teenagers to engage in both positive and negative activities, including crime. Owing to a lack of awareness, young individuals may not comprehend the consequences of their online behaviour.

To ensure children's safety online, regulatory, organisational, and educational measures have been implemented.

This chapter aims to analyse the regulations in Poland concerning the protection of children in cyberspace. It discusses the principles of child protection under civil, administrative, and criminal law, and tests the hypothesis regarding the extent and consistency of safeguarding children against emerging threats related to modern technology and universal Internet access.

A dogmatic method is employed to analyse key legal acts in the relevant field, as well as the views expressed in academic publications and case law. However, given the purpose and scope of the study, the focus is on national law. The application of regulations that provide a uniform basis for protecting Internet users throughout the European Union (e.g. the General Data Protection Regulation and the Data Services Act) is mentioned only briefly, as this issue is covered by other researchers in the project under which this article was written. Additionally, a subsidiary empirical method is used to analyse statistical data on children's use of the Internet, mobile devices, and social networking sites, as well as the risks faced by Polish children online.

2. Analysis of Key Definitions

The 1989 United Nations Convention on the Rights of the Child (CRC),[1] ratified by Poland in 1991,[2] defines "child" in Art. 1 as 'every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier'. According to Art. 3 of the Lanzarote Convention,[3] a 'child' is any person under the age of 18 years. The Budapest Convention, for the purposes of criminalising offences related to child pornography, indicates that 'the term "minor" shall include all persons under 18 years of age, but a Party may, however, require a lower age-limit, which shall

1 United Nations, 1989.
2 Journal of Laws of 1991, No. 120, item 526, as amended.
3 Council of Europe, 2007.

be not less than 16 years'.[4] The new United Nations Convention against Cybercrime, adopted by the General Assembly on 24 December 2024 in New York by resolution 79/243,[5] also sets the age limit for children at 18 years.

In international law, a precise age threshold generally defines a child as under 18 years of age. The Constitution of the Republic of Poland ("Constitution") does not define the term "child", and Polish law lacks a universal, systematic definition of the concept. Instead, Polish legislation refers to "minors", "juveniles", "adolescents", and "individuals subject to parental authority, guardianship, or custody". Simplifying, it can be assumed that, in the Polish legal system, the distinction between "child" and "adult" relies on the civil law principle of majority. According to Art. 2 of the Act of 6 January 2000 on the Ombudsman for Children,[6] a child is every human being from conception to adulthood (2.1.). The attainment of majority is determined by separate legislation (2.2.).

To determine when a person attains majority, one must refer to the Polish Civil Code (PCC).[7] In accordance with Art. 10 para. 1 PCC, 'a person shall attain majority upon reaching eighteen years of age'. Furthermore, under Art. 10 para. 2 PCC, 'A minor shall attain majority by contracting a marriage. He shall not lose the majority status in the case of the marriage being invalidated'. The legislation thus defines an adult as either 1) a person who has reached the age of 18 or 2) a person who has not yet reached 18 but is married. Only women who have reached the age of 16 and have obtained approval from the guardianship court in accordance with Art. 10 para. 1 of the Polish Family and Guardianship Code (PFGC)[8] may attain legal majority before turning 18, as per Art. 10 para. 2 PCC. Under Art. 10 § 1 of the PFGC 'a person before the age of eighteen years may not enter into marriage. However, where reasonably justified, the guardianship court may consent to the marriage of a woman who has reached sixteen years of age, if the circumstances suggest that the conclusion of the marriage will be beneficial to the new family'.

The custody of a minor and the entitlements of parents or legal representatives are regulated in the PFGC, although it does not provide a definition of the term "child".

Upon reaching the age of majority, a key legal consequence is the attainment of full legal capacity[9]. According to Art. 15 PCC, minors who have reached 13 years of age have limited capacity for juridical acts. From that moment, under Art. 20 PCC, a person with limited juridical capacity may enter into contracts of a type generally concluded in petty, everyday matters without the consent of his statutory representative. Consequently, children must reach the age of 13 before they can sign up for

4 Council of Europe, 2001.
5 United Nations, 2024.
6 Act of 6 January 2000 on the Ombudsman for Children (Unified text: Journal of Laws of 2023, item 292.)
7 Act of 23 April 1964 Civil Code (Unified text: Journal of Laws. of 2024, item 1061, as amended.)
8 Act of 25 February 1964 r. Family and Guardianship Code (Unified text: Journal of Laws of 2023, item 2809, as amended.).
9 Art. 11 of PCC.

a social media account or make small purchases (including online) independently. Without parental consent, they can also become parties to a bank account agreement and start using online banking as independent users.

As highlighted in Polish literature, the significance of reaching the age of majority extends beyond legal capacity and civil law. Upon attaining majority, an individual ceases to be subject to parental authority[10], and various provisions ensuring special protection for minors no longer apply to them[11]. In civil law, attaining adulthood grants individuals the freedom to shape their personal and financial situations, albeit at the cost of losing the special legal protection afforded to minors.[12]

The Polish Criminal Code (PCrimC, 1997)[13] specifies the age at which criminal responsibility arises, the rules for punishing young adults, and the age of the child in relation to particular offences against them. With exceptions for particularly serious offences,[14] the principles of liability in the PCrimC apply to a person who commits a prohibited act after turning 17[15]. In criminal law, distinctions are drawn between the terms "minor", "juvenile", and "young adult". Art. 115 § 10 of the PCrimC defines a young adult as an offender who has not yet reached 21 when committing the act and 24 at the time of their sentencing. A juvenile is a person who commits a criminal act after the age of 13 but before the age of 17, and is liable according to the rules set out in the Act on the Support and Rehabilitation of Juveniles.[16] The concept of a minor in criminal law is generally based on the age limit offset out in Art. 10 PCC, though this varies depending on the type of crime[17].

Under Polish law, "cyberspace" is defined as the space for processing and exchanging information created by information and communication systems, along with their links and relationships with users. This definition appears in several acts, including the Act of 29 August 2002 on Martial Law (Art. 2(1b)),[18] the Law of 21 June 2002 on the

10 Art. 92 of. PFGC.

11 e.g. Arts. 173, 442^1, 991 para 1 of PCC, and Art. 144^1 of PFGC.

12 Lutkiewicz-Rucińska, 2023.

13 Criminal Code of June 6, 1997 (Unified text: Journal of Laws of 2024, item 17, as amended.).

14 A juvenile who has committed a prohibited act, provided for in Art. 134, Art. 148 § 1, 2 or 3, Art. 156 § 1 or 3, Art. 163 § 1 or 3, Art. 166, Art. 173 § 1 or 3, Art. 197 § 3 or 4, Art. 223 § 2, Art. 252 § 1 or 2, and Art. 280, after having attained 15 years of age may be subject to the principles of liability provided for in the PCrimC if it is expedient due to the circumstances of a case and due to the degree of the perpetrator's development, his characteristics and personal conditions, especially if educational or correctional measures that had been applied previously have proven to be ineffective. In special circumstances, a juvenile who, after the age of 14 and before the age of 15, has committed a criminal act as defined in Art. 148 § 2 or 3 (aggravated murder) may be liable under the terms of the PCrimC.

15 Art. 10 para. 1 of PCrimC.

16 Act of 9 June 2022 on the Support and Rehabilitation of Juveniles (Unified text: Journal of Laws 2024, item 978.).

17 e.g. special protection for all minors in Art. 202 para 3–4c of PCrimC or only those under 15 Art. 200 para 1, paras. 3–5, Art. 200a paras. 1–2 of PCrimC.

18 Act of 30 of August 2011 on amending the Act on Martial Law and on the Competencies of the Supreme Commander (Unified text: Journal of Laws of 2022, item. 2091.).

State of Emergency in (Art. 2(1a)),[19] and the Law of 18 April 2002 on the State of Natural Disaster (Art. 3(1)(4)).[20] It was introduced by the Act of 30 August 2011, amending the Act on Martial Law and the Competencies of the Supreme Commander.[21]

The term "cybercrime" is not defined in Polish law, nor are the terms "computer crime" or "online crime". In the literature, cybercrime refers to a wide range of activities targeting the confidentiality, integrity, and availability of computer systems, networks, and data, as well as their misuse. Substantive criminal law distinguishes between attacks targeting computer systems and networks and attacks using those systems as tools.[22] More broadly, cybercrime includes acts where information technology is not the direct object but the instrument of crime (e.g. fraud, threats). From a procedural standpoint, computer-related offences include acts requiring access to information processed in information and communication technology systems.[23] Some studies differentiate between cyber-dependent crimes (a narrow or vertical approach), cyber-enabled or related crimes (a broader or horizontal approach), and, as a special category, online child sexual exploitation and abuse.[24] Given children's extensive exploration of the Internet, it is crucial to focus on criminal law protection against cybercrime.

The Act on Electronically Supplied Services[25] defines the provision of "services by electronic means" as the delivery of a service without the parties being simultaneously present (at a distance) through data transmission at the personal request of the recipient, using electronic processing devices (including digital compression and data storage), sent and received via a telecommunications network, as defined in the Electronic Communications Law.[26] For an activity to qualify as electronic service provision, it must meet three cumulative conditions: it must be performed remotely; data must be transmitted at the individual request of the recipient using electronic processing equipment; and it must be transmitted or received through a telecommunications network.

The act also defines electronic means of communication as any technical solution enabling individual remote communication through data transmission between information and communication technology systems, including (but not limited to) electronic mail.[27]

19 Act of 21 of June 2002 on the State of Emergency (Unified text: Journal of Laws of 2017, item 1928.).
20 Law of 18 of April 2002 on the State of Natural Disaster (Unified text: Journal of Laws of 2025, item 112.).
21 Journal of Laws of 2011, item 1323.
22 Gryszczyńska, 2021.
23 Adamski, 2000, p. 30.
24 Sántha, 2024, pp. 27–44; Gryszczyńska, 2024, pp. 47–78.
25 Act of 18 July 2002 on Electronically Supplied Services on Pprovision of services Services by electronic Electronic means Means (Unified text: Journal of Laws of 2024, item 1513, as amended.).
26 Act of 12 July 2024 - Electronic communications law (Journal of Laws of 2024, item 1221.).
27 Art. 2 para. 5 of Act on Electronically Supplied Services.

Notably, Polish law does not define "social media". Social media are considered electronically provided services and thus fall within the scope of the Act on Electronically Supplied Services and the Digital Services Act,[28] applicable to both service providers and users. The approach to the term "social media" in Poland is influenced by the definition of "social networking services platform" in the Network and Information Security Directive:[29] a platform enabling end-users to connect, share, discover, and communicate across multiple devices, particularly through chats, posts, videos, and recommendations. Poland has not yet implemented this Directive, despite the transposition deadline having passed.

The proliferation of electronic communication services has, unfortunately, increased the potential for criminal abuse. Such incidents can range from simple social engineering techniques to sophisticated attacks. In response, the Polish legislature in 2023 introduced the Act on Combating Abuse in Electronic Communications,[30] which defines telecommunications abuses and includes a catalogue of such abuses. "Electronic communication abuse" is defined as the provision or use of a telecommunications service or equipment contrary to its intended purpose or the law, with the aim or effect of causing harm to a telecommunications undertaking or end-user or conferring an undue advantage on the abuser or others. Both administrative provisions (e.g. blocking smishing texts and malicious websites) and criminal provisions introducing liability for artificial traffic generation[31], smishing[32], call line identification spoofing[33], and modification of address information[34] contribute to the protection of children in cyberspace.

3. The Child as a User of Information and Communication Technologies

3.1. Access to the Internet

According to the Central Statistical Office, Poland's population in 2024 is 37.63 million, of which 6.86 million are people of pre-productive age (0–17 years).[35] Of the total population, 15.1% are under 14 years old, and 20.1% are under 20.[36]

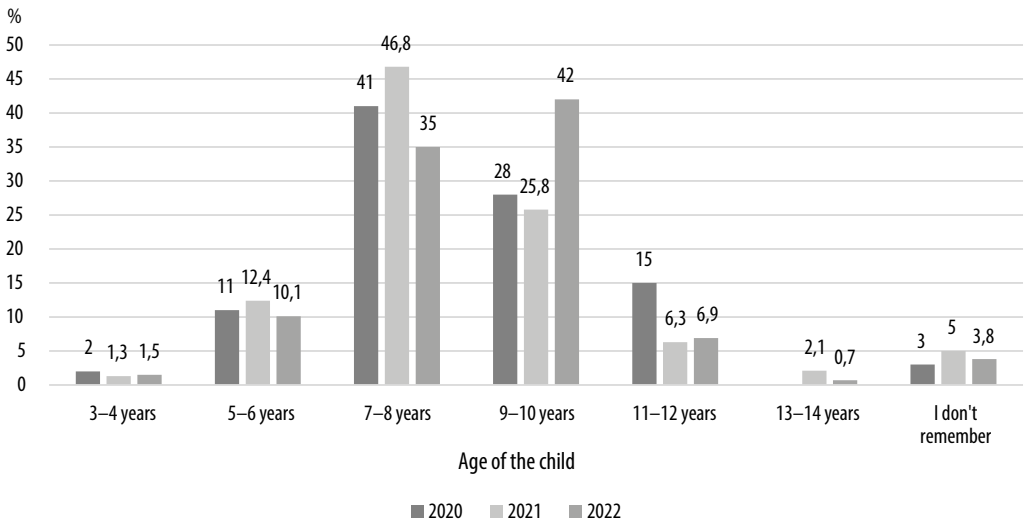
A 2024 study on the development of the information society in Poland found that 95.9% of households had access to the Internet, with the percentage varying by household type, degree of urbanisation, place of residence, and region. Households with children were more likely to have Internet access than those without.[37] In the 2022

28 European Parliament and the Council, 2022a, pp. 1–102.
29 European Parliament and the Council, 2022b, pp. 80–152.
30 Journal of Laws of 2024, item 1803.
31 Art. 29 of Act on Combating Abuse in Electronic Communications.
32 Ibid., Art. 30.
33 Ibid., Art. 31.
34 Ibid., Art. 32.
35 Główny Urząd Statystyczny, 2024a, p. 28.
36 Ibid., p. 48.
37 Główny Urząd Statystyczny, 2024b, p. 26.

edition of the Digital Economy and Digital Society Index ranking, Poland was ranked 24th among the 27 European Union Member States.[38] In Poland, young people most often access the Internet using smartphones and mobile phones (88.8%). Other frequently used devices include laptops (43.6%), desktop computers (25.4%), TVs (25.8%), and games consoles (17.4%).[39]

Regular surveys of children and parents in Poland have revealed that an overwhelming majority of children (96.9%) use smartphones. Parents largely decide on the phone's brand and service provider. Children mainly use these devices to call family and friends (86.4%), send and receive text messages, browse the web, and use various mobile applications. The most significant increase in smartphone usage among children in the 9–10 age group was observed in 2022 (Figure 1).

Figure 1. Age at which children started using their own mobile phone[40]

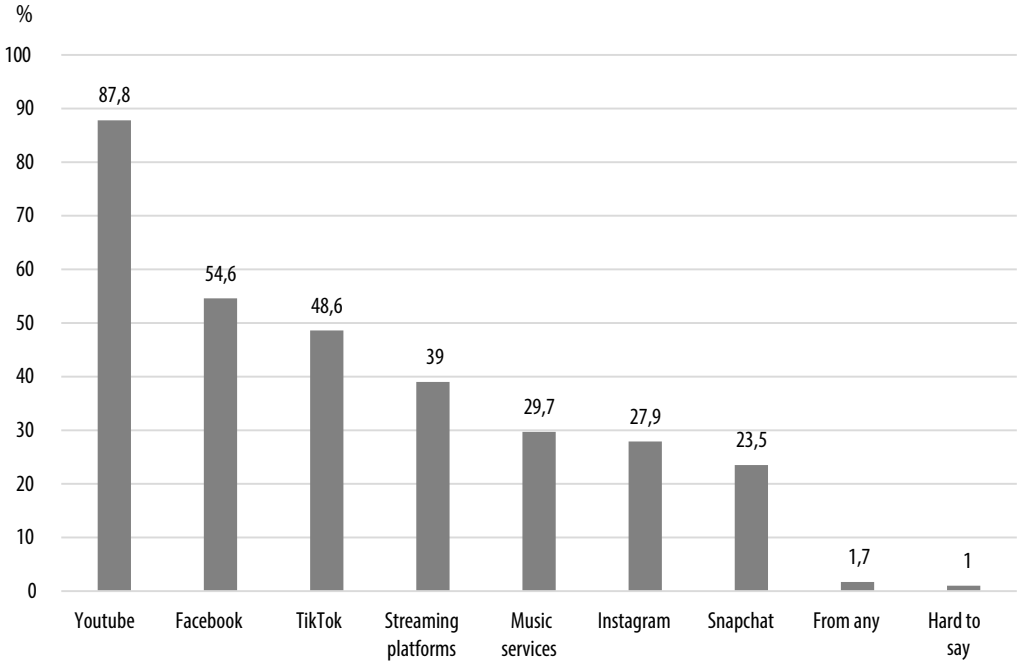


3.2. Children's Activities on the Internet

Most children use mobile phones and the Internet for reasons other than online education. Typically, children start using the Internet when they are 7–8 years old, but as many as 23.1% report going online as early as 5–6 years old. Predominantly, children use the Internet to watch YouTube videos, play games, browse websites, and engage with instant messaging and social media sites. The most commonly visited social networking sites are YouTube (87.7%), Facebook (54.6%), and TikTok (48.6%) (Figure 2).

38 Digital Economy and Digital Society Index, 2022, p. 3.
39 Lange, 2023, p. 30.
40 Source: Górecka and Czaczkowska, 2023.

Figure 2. Services and websites used by children[41]



The Scientific and Academic Computer Network (NASK) conducted a study entitled "Teenagers 3.0" on the social networking and instant messaging habits of teenagers between 2020 and 2022.[42] According to the findings, the top five platforms used by teenagers were: YouTube (87.8% in 2020, 65.4% in 2022), Facebook/Messenger (86.7% in 2020, 70.9% in 2022), Instagram (68.1% in 2020, 51.3% in 2022), Snapchat (49.6% in 2020, 41.6% in 2022), and TikTok (48.6% in 2020, 67.1% in 2022).[43]

Comparable findings emerged from a study carried out in Polish schools in early September 2022 by the Ombudsman for Children. According to this study, the number of children using social media, such as Facebook, Instagram, or TikTok, increased significantly with age. In the morning hours, only 13% of the youngest children engaged in these activities, compared to 58% of adolescents. Similar patterns were observed at midday (13%, 35%, and 58% for all age groups) and in the evening (19%, 37%, and 58%), suggesting a high probability of digital addiction among young people. Nearly half of the youngest participants (47%) reported watching TV and films on their computers in the morning, and almost one in five (18%) played computer games.

41 Ibid.

42 Teenagers 3.0. surveyed 1,733 students (from grade 7 of primary school and grade 2 of secondary school) and 893 parents and legal guardians from 61 schools in all 16 provinces in Poland. Read more: Lange, 2021, p. 5.

43 Lange, 2021, p. 25; Lange, 2023, p. 211.

The highest rates of watching TV or film viewing on computers were recorded among the youngest respondents at midday (32%) and in the evening (56%).[44]

3.3. Risks Related to Internet Access

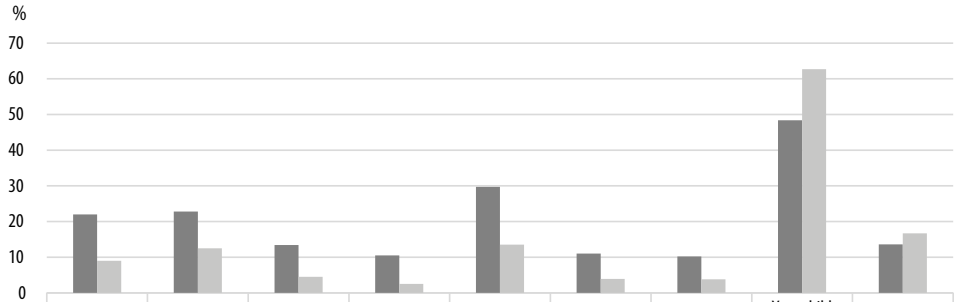
Among the most common hazards and harmful behaviours associated with children's Internet use, parents list the possibility of encountering cyberbullying (64.1%), becoming a victim of fraud (50.4%), interacting with strangers who conceal their true identity (35.5%), and developing Internet addiction (26.6%). A study conducted by NASK in 2020 and 2022 shows a steady increase in the number of hours respondents spend online. In 2020, a typical Polish adolescent spent about 12 hours a day in front of a computer or smartphone screen, including more than 7 hours of online learning due to the COVID-19 pandemic. Currently, teenagers spend an average of 5 hours and 36 minutes online each day. On weekends and holidays, this increases to an average of 6 hours and 16 minutes. Approximately 1 in 10 (11.5%) teenagers spend more than 8 hours online each day, with 1 in 5 (21.3%) reaching that figure during non-school days. A further 1 in 6 teenagers (16.9%) use the Internet intensively during nighttime hours (after 22:00). Parents often underestimate the amount of time their children spend online and fail to monitor their children's Internet use at night. Excessive consumption of virtual environments and significant engagement in online activities are so prevalent that terms such as "FOMO" (Fear of Missing Out), "problematic Internet use" (PIU), and "Internet addiction" have become widely discussed. Findings from a 2022 study using the 18-item E-SAPS18 test show that a third of teenagers (31%) display high levels of PIU, while 8 in 100 (5.1%) exhibit very high levels.[45]

Polish adolescents are not uncritical of the Internet ecosystem and do recognise its many risks. Their primary concerns include theft and the sharing of their data, loss of financial assets, hacking of smartphones and computers, and various threats related to cyberattacks. Half of adolescents express concern that their activities are tracked not only online but also in real life. Research into online violence or cybercrime reveals concerning trends: nearly half of young people have witnessed situations where their friends were attacked and insulted online (44.6%). One in three teenagers has encountered ridicule (33.2%) and humiliation (29.6%) online. Teenagers who have experienced cyberbullying were most often targeted because of their physical appearance, clothing, tastes and hobbies, political views, sexual preferences, religion, and gender. The percentage of teenagers who decide to meet an adult they met online is increasing (14.1% in 2020 and 17.9% in 2022). Alarmingly, one in four teenagers (24.5% in 2020 vs 25.3% in 2022) has not informed anyone about such incidents. One in three teenagers (32.7%) report having received nude or semi-nude photos via the Internet. More than two-thirds of young Internet users (68.4%) consider hate speech to be a problem online. Furthermore, there is a growing perception among teenagers that those who offend online go unpunished (26% in 2018 vs 51.3% in 2022).

44 Ombudsman for Children, 2023.
45 Lange, 2023, pp. 191–204.

Attention must also be drawn to the significant differences in responses between teenagers and the parents surveyed regarding experiences of online violence. Adults are not always engaged with their children's problems and may be unaware of the risks their children face (Figure 3). Seventy per cent of parents surveyed believed their child would notify them and seek their help if a problem arises. However, many teenagers do not inform anyone, with only one in four reporting problems to adults.[46]

Figure 3. Comparison of declarations regarding teenagers' experiences of online violence and parents' knowledge of the subject[47]



	Humiliation	Shaming	Scaring	Blackmailing	Insulting	Impersonating a child	Disseminating embarrassing material	Your child has not experienced violence on the Internet	Difficult to say
Teenagers	22	22,8	13,4	10,5	29,7	11	10,2	48,4	13,6
Parents	9	12,5	4,5	2,5	13,5	3,9	3,8	62,7	16,7

Significant risks include risky behaviour by children, accessing Internet pornography,[48] creating or viewing patostreams (videos posted online that depict pathological behaviour), and sexting (sending intimate images online). Analysis of age groups shows a sharp rise in exposure to Internet pornography between the ages of 11–12 and 16–17 (11.6% at primary school; 45.8% at secondary school).[49] The predominantly violent nature[50] and easy availability of Internet pornography can have a damaging effect on the developing brain, particularly during adolescence. Additionally, Internet pornography contributes to the normalisation of sexual abuse[51] and the formation of objectifying behaviour patterns.

46 Lange, 2021, pp. 82–83; Lange, 2023, pp. 52–74.
47 Source: Lange, 2021, p. 82.
48 Lange, 2022.
49 Lange, 2021, pp. 6–7.
50 Bridges et al., 2010, pp. 1065–1085.
51 Langevin and Curnoe, 2004.

It is essential to acknowledge children's vulnerability to traditional cybercrimes, including hacking, online fraud, scams, and identity theft. Nearly one in three adolescents has experienced at least one form of cybercrime, while over 10% have had unauthorised access to their email or social media accounts, or have had virtual goods, such as in-game items, stolen. More than 4% have fallen victim to identity theft or blackmail.[52] With regard to classic cybercrimes (excluding those relating to sexual freedom and morals), children are protected under the general principles of the Penal Code (PCrimC).

4. Protecting Children's Rights on the Internet

4.1. General Comments

Pursuant to Art. 72 of the Constitution,[53] the Republic of Poland guarantees the protection of children's rights. Every person has the right to demand from public authorities the protection of every child against violence, cruelty, exploitation, and demoralisation. Children deprived of parental care have the right to receive care and assistance from governmental bodies. Under Art. 48 of the Constitution, parents are entitled to raise their children in line with their own beliefs. This approach must take into account the child's level of maturity as well as their freedom of religion, conscience, and convictions. Parental rights may only be restricted or removed under specific circumstances set out in law and following a final court decision.

Like adults, children are entitled to constitutional rights such as privacy, the dissemination and acquisition of information, freedom of expression, personal data protection, and confidentiality of correspondence. The regulations governing the exercise of these freedoms and rights are outlined in specific laws. As a subject of rights, a child is entitled to the protection of his or her personal property, as defined in the PCC, as well as the special protection of criminal law under the PCrimC. The age of a child victim may also determine criminalisation and be considered an aggravating circumstance for the severity of punishment under the PCrimC. In civil, criminal, or administrative proceedings, a legal representative, such as a parent or the minor's permanent custodian (e.g. a foster carer), typically represents the child.

In accordance with Arts. 99 et seq. of the PFGC, if neither parent can represent a child under parental authority, the guardianship court shall appoint a child representative. The child representative is authorised to perform all activities relating to the case, including appeals and the execution of rulings. A child representative may be an attorney-at-law or legal counsel who has special knowledge of issues relating to the child, or who has completed training regarding the principles of representing a child and the rights or needs of a child. Where the complexity of the case does not

52 Lange, 2023, pp. 95–100.

53 Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws No. 78, item 483, as amended.)

require such expertise, particularly where the guardianship court determines the nature of the activities, the child representative may also be a person holding a degree in law and demonstrating familiarity with the child's needs. The activities of the child representative are subject to ongoing supervision by the guardianship court, which maintains oversight of the child's actions.

It is also important to highlight the amendments made to existing legislation in 2023, which aim to strengthen the protection of children's rights. Pursuant to the Act of 28 July 2023 amending the Act – Family and Guardianship Code and certain other acts,[54] an amendment to the Act of 13 May 2016 on Counteracting the Risk of Sexual Offences and Protection of Minors entered into force on 15 February 2024. The scope of the Act was expanded, and provisions on the general protection of minors were introduced. The Act establishes specific measures for protection against the threat of sexual offences and specific measures for the protection of minors, including the obligation to introduce standards for the protection of minors and measures to protect them from abuse. According to the introduced provisions, to create conditions for the effective protection of minors from harm, the Council of Ministers is to adopt the National Plan against violence to the detriment of minors and the National Plan against crimes against sexual liberty and vice to the detriment of minors. The national plans are to include, *inter alia:* activities to prevent violence and crimes against sexual freedom and morality against minors; organisation of a system of material, psychological, medical, and legal support for victimised minors; dissemination of information about available support and assistance for victims and their families; activities in the field of rehabilitation and work with perpetrators; ways of involving minors in the development and implementation of the national plans.

The first National Plan against Crimes against Sexual Liberty and Vice to the Harm of Minors for 2023–2026 was adopted on 17 October 2023 and is annexed to the resolution of the Council of Ministers.[55] The provisions of the Law on Counteracting the Risk of Sexual Offences and Protection of Minors also have important implications for the protection of children's rights in cyberspace.

4.2. Right to Privacy and Right to Be Forgotten

Research conducted in 2010 by AVG Technologies found that, on average, children acquire a digital identity by the age of six months.[56] Additionally, 81% of two-year-olds have a digital footprint, and 23% of mothers have uploaded photos of their children's prenatal scans online, creating a digital footprint for their child even before birth.[57]

Art. 47 of the Constitution grants every individual the legal right to the protection of his or her privacy, family life, honour, and good name, as well as the right to determine his or her personal life. Art. 49 of the Constitution ensures the freedom

54 Act of 28 July 2023 amending the Act - Family and Guardianship Code and certain other act (Journal of Laws of 2023, item 1606.)
55 Council of Ministers, 2023b.
56 Brosch, 2016, p. 226.
57 AVG, 2010.

and confidentiality of communication. The constitutional basis for the protection of personal data is found in Art. 51 of the Constitution, which states that no one may be obliged to disclose personal information except on the basis of a law.

A child, like any adult, has the right to the protection of his or her privacy, including his or her image, which is considered a personal interest under Art. 23 of the PCC. The image is safeguarded through the PCC, the Copyright and Related Rights Act,[58] the Personal Data Protection Act,[59] and, particularly for children, the PFGC. Under Art. 81 para. 1 of the Copyright Act, permission is required from the depicted individual (whether an adult or a child) for the dissemination of their image. As children lack full legal capacity, their rights are exercised by their guardians or parents until they attain legal majority. Therefore, any authorisation for the use of a child's image must be granted by their legal guardians or parents. When publishing images of children online, it is important to consider that, while legally it is the parents who have the authority to make their children's images available, the PFGC mandates that they must act in the best interests of the child's welfare and well-being.

The age at which a child is permitted to use online services varies depending on the policies of individual platforms (usually 13 or 16) and on the legislation regarding the age at which a child acquires limited legal capacity. The conditions for a child's consent in the case of information society services are set out in Art. 8 of the General Data Protection Regulation. Furthermore, children's rights are also covered under Art. 17 of this regulation, which establishes a general basis for the right to be forgotten.

4.3. Right of Access to Information and Right to Education

The right to information and education in Poland is guaranteed by the Constitution, with the exercise of these rights regulated by specific laws. Access to information is subject to the same provisions for all subjects of rights and freedoms. Art. 54 of the Constitution guarantees the freedom to express opinions and to acquire and share information. Preventive censorship of social media and press licensing is prohibited. In addition, according to Art. 61 of the Constitution, citizens have the right to acquire information concerning the activities of public authorities and individuals in public positions. This right also extends to obtaining information on the activities of organs of economic and professional self-government, as well as other persons and organisational units, to the extent that they perform public authority tasks and manage communal property or State Treasury property.

According to the Act on Access to Public Information,[60] every individual, regardless of citizenship status, has the right of access to public information. The primary means of access is a proactive, non-request mode, allowing public access to official documents and information through publication in the Public Information Bulletin, which serves as the official tele-information platform, presented in a unified system of

58 Unified text: Journal of Laws of 2025, item 24.
59 Unified text: Journal of Laws of 2019, item 1781.
60 Unified text: Journal of Laws of 2022, item 902.

pages within the tele-information network. The process for acquiring information not published online in the Public Information Bulletin is simplified: anyone, including a child, can apply for access to public information. Since 2012, the law has been published electronically in Poland[61] on the website www.dziennikiurzedowe.gov.pl. Both children and young people are provided with access to specific information, as well as the freedom to acquire and distribute information based on general principles.

According to Art. 70 of the Constitution, all individuals have the right to education. Compulsory education is mandated until the age of 18 and is governed by educational law.[62] In Poland, public schools provide education free of charge. Public authorities must ensure that citizens have universal and equal access to education. Thus, the authorities establish and maintain systems of financial and organisational assistance for pupils and students.

Only by ensuring appropriate education, fostering digital competences, incident response, and the appropriate attitudes can we guarantee the protection of children's rights in cyberspace. It is therefore worth referencing the specific regulations concerning the development of digital competences in Poland.

Digital competence, comprising the knowledge, skills, and attitudes related to digital technologies, significantly affects individual and societal well-being and welfare. A crucial aspect of digital competence is the practical ability to use digital media, devices, and technologies in a skilful, informed, and responsible way for learning, work, and leisure in both private and public spheres. According to the Digital Competence Framework for Citizens, digital competence includes skills in information and data handling, communication and collaboration, digital content creation, and security and problem-solving.[63]

Research conducted by various entities at different times shows that the digital literacy of the Polish population is below the European Union average. According to the Digital Economy and Society Index indicators for 2024[64], 44% of people aged 16–74 in Poland have at least basic digital skills, while only 20% have above-basic digital skills. Additionally, UKE research from the end of 2020 reveals that 27% of Polish children start using the Internet before the age of six,[65] before beginning formal education.

Although the 2023 IT Fitness Test results indicate a higher average score for digital competences among children and young people compared to 2022, primary school pupils achieved only 46%, and secondary school pupils 43% of correct answers.[66]

Considering the significance of developing digital competences among children, Resolution No. 24 of the Council of Ministers on 21 February 2023 introduced a governmental initiative titled the Digital Competence Development Programme,[67] which

61 Unified text: Journal of Laws of 2019, item 1461.
62 Unified text: Journal of Laws of 2024, item 737, as amended.
63 Vuorikari Kluzer and Punie, 2022.
64 European Commission, 2022.
65 UKE, 2021.
66 Cyfrowa Polska, 2023.
67 Council of Ministers, 2023a.

will be active until 2030. For pupils, the objectives of the Programme for the Development of Digital Competences include: 1. preparing children and young people to function safely, consciously, and creatively in the information society; and 2. creating an environment conducive to the development of advanced digital competences and digital talents, while also considering the need to increase the participation of girls in areas related to digital technologies. This programme considers statistics on Internet and mobile device usage by children under six, and includes pre-school children in preparation for safe, informed, and creative functioning in the information society. It envisages developing a training programme, lesson plans, and educational materials for pre-school teachers to prepare them to work effectively with both children and parents.

Support for developing digital skills has two recognisable dimensions: technological and educational/developmental, as defined in the Digital Competence Development Programme. Both public and private entities undertake initiatives aimed at promoting digital literacy among children, adolescents, and their parents. Training courses and educational materials for parents, teachers, and schools are made available electronically as part of the activities of various institutions, including the Ministry of Digitalisation, NASK, and the Dajemy Dzieciom Siłę Foundation.[68] Many of the training courses offered address different professional groups and provide various forms of in-service training for teachers, covering issues such as cybersecurity, offensive and illegal content online, cyberbullying, and countering child sexual abuse.

Particularly noteworthy is the preparation of lesson scenarios for teachers by institutions dealing with the protection of children on the Internet, which can be used at school to develop children's cyber hygiene and their resilience to various threats.[69] It is also important to build the knowledge and skills of parents, for whom dedicated educational materials are also being developed, such as the parent guides Cyberbullying – Turn on the Bullying Blocker,[70] FOMO and Abuse of New Technologies,[71] Sexting and Naked Pictures: Your Child and Negative Online Behaviour,[72] Sharenting and Your Child's Online Image,[73] and Harmful Content on the Internet: I Don't Accept, I React!,[74] which were co-produced by the Ministry of Digitalisation and the NASK Academy as part of the "Don't Lose Your Child Online" campaign.

68 See: https://www.gov.pl/web/baza-wiedzy/cyberedukacja (Accessed: 29 January 2025); Borkowska, 2020; https://cyberprofilaktyka.pl/ (Accessed: 29 January 2025); https://www.saferinternet.pl/ (Accessed: 29 January 2025); https://dyzurnet.pl/dla-rodzicow-i-opiekunow (Accessed: 29 January 2025).

69 See: https://www.saferinternet.pl/materialy-edukacyjne/scenariusze-zajec.html (Accessed: 29 January 2025).

70 Borkowska, 2020.

71 Witkowska, 2020.

72 Kwaśnik, 2020.

73 Borkowska and Witkowska, 2020.

74 Piechna, 2020.

4.4. Right to Be Safeguarded From Abuse

There are numerous risks associated with children's use of the Internet. Among the most common threats and hazardous behaviours identified by parents are the possibility of experiencing cyberbullying (64.1%), becoming a victim of fraud (50.4%), and contact with strangers hiding their real identity (35.5%).[75] However, the risks with the greatest severity to which children are exposed in cyberspace include sexual exploitation and sexual abuse.[76] These offences are defined in the provisions of the PCrimC. Children are generally protected as victims in relation to classic cybercrimes (fraud, computer fraud, hacking, stalking, and identity theft). Special protection applies to offences involving sexual abuse.

Statistical analysis of judgments passed by common courts in cases of offences under Chapter XXV of the PCrimC against minors during the years 2018–2021 reveals that 8,524 proceedings for violations of sexual freedom were carried out in first instance courts. Of these, 7,870 proceedings were conducted at the district court level, while 654 proceedings were conducted at the county court level. A total of 7,698 perpetrators were convicted by the courts. In 251 instances, proceedings were terminated, and in 76 instances, proceedings were conditionally discontinued. Moreover, 492 suspects were acquitted, and punishment was waived for seven offenders.[77]

In its rulings, the Supreme Court affirms that the aim of protecting minors against sexual exploitation is to safeguard their morality and ensure their proper moral and physical development.[78]

In Poland, one of the offences subject to criminalisation is grooming. According to Art. 200a. para. 1 PCrimC, whoever – with the purpose of committing a crime provided for in Art. 197 § 3 section 2 or Art. 200, as well as producing or recording pornographic content – establishes contact with a minor under 15 years of age via a telecomputer system or telecommunications network, aiming to induce him into a meeting by misleading him, exploiting his error or incapacity to fully understand the situation, or by using an unlawful threat, is subject to a penalty of deprivation of liberty for up to three years.

According to Art. 202 para. 3 PCrimC, whoever – with the purpose of dissemination – produces, records or imports, stores or possesses, or disseminates or displays pornographic content involving a minor, or pornographic content involving violence or the use of an animal, is subject to a penalty of deprivation of liberty for between two and fifteen years.

Of particular significance is the disparity in the age of the victim in relation to the offences established under Arts. 200 or 200a PCrimC and Art. 202 para. 3 PCrimC. Since 2014, there has been enhanced protection for all minors. Furthermore, the

75 Górecka and Czaczkowska, 2023.
76 Staciwa, 2023.
77 National Plan Against Crimes against Sexual Freedom and Vice against Minors 2023–2026.
78 Supreme Court judgment of 12 September 1997, V KKN 306/97.

consent of the minor is irrelevant for the existence of the offence under Art. 200 PCrimC.[79]

According to the case law of the Supreme Court, "pornographic content" within the meaning of Art. 202 of the Criminal Code is the presentation of human sexual activities (in particular the depiction of human sexual organs in their sexual functions), whether in a fixed form (e.g. film, photographs, magazines, books, or images) or not (e.g. live shows), and both in a dimension not contradictory to their biological orientation and human sexual activities contradictory to socially accepted patterns of sexual behaviour.[80] Criminal liability for disseminating child pornography on the Internet depends not on the specific number of users who have viewed such content, or whether this number is significant, but on the manner in which the pornographic files were downloaded and made available via applicable software, providing an undetermined number of people with access to them.[81]

Given the purpose of this research, when discussing responsibility for abuse, the focus is on those criminal acts where the child is particularly protected. However, the general provisions of criminal law, which provide the basis for criminal liability regardless of the age of the victim, must not be overlooked. In Poland, the basic provisions constituting the grounds for criminal liability for cybercrime are contained in Chapter XXXIII of the Criminal Code, titled Offences Against the Protection of Information. Cyber-dependent crimes are specifically addressed in the Arts. 267, 268 para. 2, 268a, 269, 269a, and 269b of the PCrimC. Criminal proceedings for cybercrime cases may also be initiated based on classic offences against property[82]. A child, like any other person, can also claim protection against defamation or insult, whether committed in the real world or online[83].

New challenges and the discovery of new vulnerabilities and attack scenarios are also prompting legislative action. It is worth mentioning a new and important regulation in Poland limiting the effects of fraud in electronic communication. Attacks based on the impersonation of telephone numbers of public officials, police units, and banks (caller line identification spoofing) have led to the initiation of a legislative process to combat the abuse of electronic communications. On 28 July 2023, the law on combating abuse in electronic communication was enacted, introducing not only new types of criminal acts and criminal sanctions for sending messages impersonating another entity but also a regulation of an administrative nature relating to the blocking of short text messages (SMS) containing content included in the pattern of messages deemed to be abusive. This law is intended to provide a basis not only for combating smishing, vishing, and caller line identification spoofing but also for blocking domain names impersonating other entities. From a child protection perspective,

79 Supreme Court decision of 17 November 2021, II KK 490/21.
80 Judgment of the Supreme Court of 23 November 2010, IV KK 173/10.
81 Decision of the Supreme Court of 1 September 2011, V KK 43/11.
82 Art. 286 para. 1 of the PCrimC for fraud, Art. 279 § 1 of the PCrimC for burglary, and Art. 287 para. 1 of the PCrimC for computer fraud.
83 Arts. 212 and 216 of the PCrimC.

this law will reduce children's exposure to phishing sites and help reduce the risk of phishing, hacking, and identity theft by blocking SMS messages with malicious links and the ability to access sites that steal login credentials.

4.5. Right to Freedom of Expression and Right to Be Heard

Among the rights of personal freedoms, the Constitution guarantees everyone the freedom to express his or her opinions and to obtain and disseminate information[84]. At the same time, one of the limits of freedom of expression is the protection of personal rights of third parties, which derive from the inherent and inalienable dignity of the human being.[85][86]

The right to speak is a procedural guarantee granted to parties and participants in legal proceedings. This right comprises the liberty to impart one's views, the freedom to address the court, the authority to decide, as well as the entitlement to seek, receive, and impart information. Art. 72 para. 3 of the Constitution establishes the constitutional criterion for the child's involvement in legal proceedings, requiring public authorities and individuals responsible for the child to listen to and consider the child's views when making decisions regarding the child's rights. When formulating a request for a hearing of evidence, it is necessary to indicate the purpose and rationale for applying Art. 216^1 para. 1 of the Polish Code of Civil Procedure (PCCP)[87] in a given case, as indicated in legal precedents. Such a hearing does not constitute an examination as a witness. To consider the child's opinion (as set out in Art. 216^1 para. 2 of the PCCP), the court must consider the child's circumstances and the extent to which their reasonable wishes can be taken into account. This provision should only be applied to situations where the child's opinion is legally relevant. A purposive interpretation of this provision is necessary.[88]

In criminal proceedings involving a child victim, their rights are exercised by a statutory representative, such as a parent or legal guardian. However, the Supreme Court resolution of 30 September 2010[89] stipulated that if one parent is accused, the other parent acting as a legal representative cannot exercise the rights of the minor as a victim. In this scenario, a legal representative may be appointed for the child from the very beginning of the proceedings.

Interviewing a minor victim carries the risk of secondary victimisation. Therefore, like any witness, the interviewed minor victim has certain rights and obligations during this process. These rights can be divided into two groups. The first group includes those deriving directly from the Code of Criminal Procedure,[90] such as the right to refuse to testify and the right to evade answering a question in the case of a

84 Art. 54 of the Constitution.
85 Ibid., Art. 30.
86 Judgment of the Supreme Court of 8 December 2020, I NSNc 44/20.
87 Journal of Laws of 2023, item 1550, as amended.
88 Judgment of the Court of Appeal in Gdańsk of 20 January 2016, V ACa 607/15.
89 Resolution of the Supreme Court of 30 September 2010, I KZP 10/2010.
90 Journal of Laws of 2022, item 1375, as amended.

particularly close relationship with a suspect or defendant. The second group includes those deriving indirectly from the provisions of the Code of Criminal Procedure and the literature on questioning a child under Art. 185a of the Code of Criminal Procedure, namely the right to prepare the child for questioning and the right to protection against secondary victimisation. Among the obligations imposed on the minor are the obligation to appear and remain at the disposal of the trial authority, as well as the obligation to give evidence and tell the truth. Statistics from the Ministry of Justice show that the number of children being questioned under Art. 185a of the Polish Code of Criminal Procedure is increasing year by year. This indicates that the justice authorities consider the child to be a reliable source of evidence.[91]

5. Institutions Set Up in Poland to Protect Children's Rights in the Digital World

The enforcement of children's rights in Poland takes place within the framework of laws that address different areas of life (education, healthcare, social benefits, and family law) and programmes, such as the National Programme for Counteracting Domestic Violence 2014–2020, the National Plan for Combating Crimes Against Sexual Liberty and Vice Against Minors for 2023–2026, and the Digital Competence Development Programme.[92] The tasks provided for in the various area laws are carried out by different public entities, and it would be beyond the scope of this study to refer to all the institutions responsible for guaranteeing the protection of children and the realisation of their rights, both in general and in the digital world. The focus here is on the key actors and institutions dedicated to child protection and protecting children from cyber threats.

In the Polish legal system, the guardian of children's rights, as defined by the Constitution, the CRC, and other legal regulations, is the Ombudsman for Children, whose status is regulated by the Act of 6 January 2000 on the Ombudsman for Children.[93]

The Ombudsman, in accordance with this Act, takes measures to ensure the full and harmonious development of the child, respecting his or her dignity and subjectivity. The Ombudsman acts to protect the rights of the child, in particular: 1. the right to the protection of life and health; 2. the right to family upbringing; 3. the right to decent social conditions; and 4. the right to education. In addition, the Ombudsman takes action to protect the child from violence, cruelty, exploitation, demoralisation, neglect, and other forms of ill-treatment. Special care and assistance are given to children with disabilities. The Ombudsman also promotes children's rights and methods of protecting them. The Ombudsman takes the measures provided for in the Act on his own initiative, especially considering information from citizens or their

91 Osiak, 2016.
92 Council of Ministers, 2023a.
93 Unified text: Journal of Laws of 2023, item 292.

organisations indicating violations of children's rights or welfare. Within his competence, the Ombudsman for Children may: investigate any case on the spot, even without prior notice; request explanations, information, or access to files and documents from public authorities, organisations, or institutions; report to and participate in proceedings before the Constitutional Court initiated at the request of the Ombudsman or in cases of constitutional complaints concerning the rights of the child; file petitions with the Supreme Court to resolve discrepancies in the interpretation of legal provisions concerning the rights of the child; file a cassation or a cassation appeal against a final decision in accordance with the procedure and principles laid down in separate regulations; request the initiation of civil proceedings and participate in pending proceedings, with the rights of a public prosecutor; participate in pending juvenile proceedings, with the rights of a public prosecutor; request the initiation of pre-trial proceedings in criminal cases by an authorised prosecutor; request the initiation of administrative proceedings, file appeals with the administrative court, and participate in such proceedings, with the rights of a public prosecutor; file a petition for punishment in misdemeanour proceedings, in the manner and according to the rules set forth in separate regulations; and commission studies and prepare expert reports and opinions.

The Ombudsman may also request the competent authorities, organisations, or institutions to act on behalf of a child within their respective areas of competence. The authority, organisation, or institution to which the Ombudsman has addressed a complaint on behalf of a child must inform the Ombudsman without delay, and in any case within 30 days, of the action taken or the position adopted. Every child is also protected as a person and as a citizen. The protection of the freedoms and rights of the individual and the citizen laid down in the Constitution and other legal acts, including the implementation of the principle of equal treatment in Poland, is the responsibility of the Ombudsman (Public Defender of Rights), whose duties and powers are regulated by the Act of 15 July 1987.[94] In matters concerning children, the Ombudsman cooperates with the Ombudsman for Children.

Given the identified risks and the regulations guaranteeing the protection of children from threats, attention should be drawn to the tasks of the teams operating within the Scientific and Academic Computer Network. Pursuant to the Act of 5 July 2018 on the National Cyber Security System,[95] the National Cyber Security System includes, among others, the Computer Security Incident Response Team (CSIRT), which operates at the national level and is led by the Scientific and Academic Computer Network – National Research Institute. According to Art. 26(6)(3), the tasks of the CSIRT NASK include providing a telephone line or Internet service for the reporting and analysis of incidents involving the distribution, dissemination, or transmission of child pornography by means of information and communication technologies, as referred to in Directive 2011/93/EU of the European Parliament and of the Council of

94 Unified text: Journal of Laws of 2024, item 1264, as amended.
95 Unified text: Journal of Laws of 2024, item 1077, as amended.

13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA.[96] This task is carried out by the CSIRT NASK as part of the Dyżurnet.pl team, which acts as a contact point for reporting illegal content on the Internet, especially related to child sexual abuse. The mission of the Dyżurnet.pl team is to take action to create a safe Internet. As a national hotline team, Dyżurnet is a member of the Association of Internet Hotline Providers (INHOPE). More than 50 hotlines from all over the world are members of INHOPE, and its activities are supported by Interpol, Europol, the Virtual Global Taskforce, the European Financial Coalition, INSAFE, ECPAT, and various global IT companies. Dyżurnet is supported by an Advisory Committee comprising representatives from government, the judiciary, and non-governmental organisations. Dyżurnet also cooperates with the police and helplines: 800 100 100 (a helpline for teachers and parents) and 116 111 (a helpline for children and young people run by the Dajemy Dzieciom Siłę Foundation).[97]

In order to take appropriate measures and ensure cooperation between the representatives of the various institutions, Resolution No. 204 of the Council of Ministers of 17 October 2023 was published on 16 November 2023, adopting the National Plan against Crimes Against Sexual Liberty and Vice to the Detriment of Minors for 2023–2026.[98]

The sexual exploitation of children is an intolerable phenomenon that must not be overlooked. Measures should be taken to prevent sexual offences and reduce situations where harm can be inflicted upon children. Law enforcement agencies, particularly the police and the Public Prosecution Service, have a crucial role in safeguarding the well-being of minors. In July 2022, the Central Bureau for Combating Cybercrime was established in Poland. In August of the same year, the Department for Cybercrime and Informatisation at the National Prosecutor's Office was established, which, among other tasks, coordinates activities in proceedings related to sexual abuse of minors in cyberspace. These activities lead to ongoing pre-trial proceedings, resulting in indictments and subsequent convictions of individuals who have committed crimes against minors. Simultaneously, there has been a rise in the number of proceedings and indictments concerning crimes related to the sexual abuse of minors more broadly. The Central Bureau for Combating Cybercrime, in collaboration with the Public Prosecutor's Office, conducts coordinated efforts to combat, among other things, the sexual exploitation of minors and the distribution of materials depicting the sexual exploitation of minors.[99] An example of measures to protect children from sexual exploitation is the coordinated arrests of persons linked to paedophile communities, organised as part of the so-called Action Week. In several coordinated operations carried out between 2022 and 2024 by the Central Bureau for

96 European Parliament and the Council, 2011, pp. 1–14.
97 Prusak-Górniak and Silicki, 2019, p. 254.
98 Council of Ministers, 2023b.
99 Centralne Biuro Zwalczania Cyberprzestępczości, 2023.

Combating Cybercrime and the Department for Cybercrime and Informatisation of the National Prosecutor's Office, several hundred people were arrested.[100] In an operation carried out in October 2024 alone, more than 400 officers from the Central Bureau for Combating Cybercrime, in collaboration with the Department for Cybercrime and Informatisation, conducted 112 searches, resulting in the seizure of more than 7,500 devices of various types (telephones, computers, laptops, discs, memory sticks, etc.). In total, more than 1,141,000 images and video files were seized, and 75 people aged between 16 and 78 were arrested on suspicion of possessing and distributing child sexual abuse content.[101]

6. Conclusion and Proposals

Ensuring comprehensive protection of children's rights in cyberspace requires a holistic approach, including maintaining consistency among regulations in civil, criminal, and administrative law to effectively safeguard these rights. Another important measure is to ensure consistency in regulations concerning various aspects of children and young people's activities, including education, parental care, the rights and responsibilities of children as individuals and citizens, and as users of online services.

In Poland, to ensure the effective protection of minors on the Internet, consultations have been held with experts, and groups consisting of representatives from various backgrounds, including law enforcement agencies and non-governmental organisations, have been established to promote collaborative efforts and offer support in protecting minors online, including operating helplines for children.

The years 2022–2024 saw extensive discussions on children's rights in Poland, and measures were taken that were evaluated both negatively and positively. Measures taken to protect children from the threat of sexual offences can be assessed positively. The extension of the scope of the law against sexual offences to encompass the general protection of minors is a step towards a more comprehensive approach. It remains to be seen whether these changes have increased the level of protection for children in cyberspace.

The adoption of the National Plan to Combat Crimes Against Sexual Liberty and Vice Against Minors 2023–2026 should be considered an important step in combating behaviours detrimental to the safety and well-being of minors. This document sets out the most important goals and tasks of individual public authorities. Importantly, the implementers of the various objectives set out in it are identified, along with the deadlines for their implementation.

However, one of the foremost challenges children currently face is hate speech and cyberbullying, which are frequently perpetrated by their peers. Predators who

100 Prokuratura Krajowa, 2023.
101 Przemysław, 2024.

are shielded from repercussions, as they do not have to confront their victims in person, often disregard the harm caused. The antisocial conduct of children is regularly overlooked by their parents and educators, leading to the normalisation of such behaviour. Abused children often cannot cope with the negative consequences of the attacks. They are frequently deprived of support from psychologists (27% of school psychologist posts in Poland are vacant). In addition, child psychiatry in Poland is in a serious crisis. Insufficient social education on the mental health of children and adolescents, inadequate psychological support and teaching in schools and educational institutions, difficulties for parents and guardians in accessing the requisite help, and a lack of awareness that such assistance may be needed have resulted in an increasing number of suicides committed by children. According to data from the National Police Headquarters, 2,093 children and young people aged between 7 and 18 attempted suicide in 2022. One hundred and fifty-six cases resulted in fatalities, whereas, in 2021, approximately 1,500 suicide attempts were made, and in 2020, there were fewer than 1,000.[102] A comprehensive approach to protecting children in cyberspace should include safeguarding their overall well-being, including their mental health.

It is extremely important to include cyber rights and cyber threats in educational activities. However, education must not only be directed at children, young people, and teachers. Parents, who are often unaware of the risks and unfamiliar with the various methods of keeping their children safe in the virtual world, need to be educated first and foremost.

In order to protect children from pathological content (such as patostreaming[103] and child sexual abuse material), every Internet user needs to develop the habit of reporting violations of the law. Websites should be obliged to filter and block offending content, under penalty of heavy fines or liability for aiding and abetting a crime. Many platforms not only fail to proactively moderate content but also fail to respond to reported infringements. Given the global nature of the providers of such services, there is a need to act internationally – beyond the European Union. The Act on Combating Abuse in Electronic Communications, introduced in Poland, does not apply to all illegal content but only to phishing sites. However, it demonstrates that the creation of effective protection mechanisms requires the cooperation of actors within the national cybersecurity system, telecommunications providers, and all users.

102 The number of suicide attempts by children and adolescents is increasing, 2023, see: Medycyna Praktyczna, 2023).

103 "Patostream": pathological stream is a type of live broadcast where the host engages in shocking, dangerous, humiliating, or otherwise controversial actions, often involving themselves or other persons.

Bibliography

Adamski, A. (2000) *Prawo karne komputerowe*. Warsaw: C.H. Beck.

AVG (2010) 'Would you want a digital footprint at birth?' [Online]. Available at: https://www.avgdigitaldiaries.com/image/12794514549 (Accessed: 29 January 2025).

Borkowska, A. (2020) *Cyberprzemoc – Włącz Blokadę Na Nękanie: Poradnik dla Rodziców*. Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://www.gov.pl/web/niezagubdzieckawsieci/do-poczytania (Accessed: 29 January 2025).

Borkowska, A., Witkowska, M. (2020) *Sharenting and your child's online image. A guide for parents (Sharenting i wizerunek dziecka w sieci. Poradnik dla rodziców).* Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://www.gov.pl/web/niezagubdzieckawsieci/sharenting-i-wizerunek-dziecka-w-sieci (Accessed: 29 January 2025).

Bridges, A., et al. (2010) 'Aggression and Sexual Behavior in Best Selling Pornography Videos: A Content Analysis Update', *Violence Against Women*, 16(10), pp. 1065–1085; https://doi.org/10.1177/1077801210328666.

Brosch, A. (2016) 'When the Child is Born into the Internet : Sharenting as a Growing Trend among Parents on Facebook', *The New Educational Review*, 43(1), pp. 225–235; https://doi.org/10.15804/tner.2016.43.1.19.

Centralne Biuro Zwalczania Cyberprzestępczości (2023) 'Operacja Carlos – kolejne uderzenie CBZC w przestępczość o podłożu pedofilskim', *CBZC online*, 3 November [Online]. Available at: https://cbzc.policja.gov.pl/bzc/aktualnosci/214,Operacja-CARLOS-kolejne-uderzenie-CBZC-w-przestepczosc-o-podlozu-pedofilskim.html (Accessed: 29 January 2025).

Council of Europe (2001) 'Convention on Cybercrime', *Council of Europe Treaty Series,* No. 201 [Online]. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 29 January 2025).

Council of Europe (2007) 'Convention on Protection of Children against Sexual Exploitation and Sexual Abuse', *Council of Europe Treaty Series,* No. 201 [Online]. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201 (Accessed: 29 January 2025).

Council of Ministers (2023a) 'Resolution No. 24 of the Council of Ministers of 21 February 2023 on the establishment of a government programme called "Digital Competence Development Programme"', Legal Monitor of 2023, item 318.

Council of Ministers (2023b) 'Resolution No. 204 of the Council of Ministers of 17 October 2023 on the adoption of the National Plan against Crimes against Sexual Liberty and Vice to the Harm of Minors for 2023-2026', *Legal Monitor of 2023*, item 1235.

Cyfrowa Polska (2023) 'Wyniki IT Fitness Test 2023: Uczniowie dobrze radzą sobie w sieci, problem mają z narzędziami biurowymi', *Cyfrowa Polska,* 23 November [Online]. Available at: https://cyfrowapolska.org/pl/wyniki-it-fitness-test-2023-uczniowie-dobrze-radza-sobie-w-sieci-problem-maja-z-narzedziami-biurowymi/ (Accessed: 29 January 2025).

European Commission (2022) 'Digital Economy and Society Index (DESI) 2022 – DESI country profile: Poland' [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (Accessed: 29 January 2025).

European Parliament and the Council (2011) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA.

European Parliament and the Council (2022a) Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

European Parliament and the Council (2022b) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

Główny Urząd Statystyczny (2024a) *Rocznik Demograficzny 2024*. Warsaw: GUS [Online]. Available at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/rocznik-demograficzny-2024,3,18.html (Accessed: 29 January 2025).

Główny Urząd Statystyczny (2024b) *Społeczeństwo informacyjne w Polsce w 2024 r.* Warsaw: GUS [Online]. Available at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/rocznik-demograficzny-2024,3,18.html (Accessed: 29 January 2025).

Górecka, M., Czaczkowska, J. (2023) 'Jak młodzi użytkownicy korzystają z usług telekomunikacyjnych – wyniki badania dzieci i rodziców', *Urząd Komunikacji Elektronicznej,* 7 February [Online]. Available at: https://www.uke.gov.pl/blog/jak-mlodzi-uzytkownicy-korzystaja-z-uslug-telekomunikacyjnych-wyniki-badania-dzieci-i-rodzicow,70.html (Accessed: 29 January 2025).

Gryszczyńska, A. (2021) 'Cyberprzestępczość.' in Szpor, G., Grochowski, L. (eds.) *Wielka Encyklopedia Prawa – Tom XXII: Prawo informatyczne*. Warsaw: Fundacja Ubi Societas Ibi Ius, pp. 89–90.

Gryszczyńska, A. (2024) 'The scope of criminalisation of cybercrime in Poland' in Gryszczyńska, A. (ed.) *Cybercrime*. Warsaw: Instytutu Wymiaru Sprawiedliwości, pp. 47–78 [Online]. Available at: https://wydawnictwo.iws.gov.pl/wp-content/uploads/2024/12/GRYSZCZYNSKA-Cybercrime_www.pdf (Accessed: 29 January 2025).

Kwaśnik, A. (2020) *Sexting i nagie zdjęcia – Twoje dziecko i negatywne zachowania online. Poradnik dla rodziców*. Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://www.gov.pl/web/niezagubdzieckawsieci/sexting-i-nagie-zdjecia-twoje-dziecko-i-negatywne-zachowania-online (Accessed: 29 January 2025).

Lange, R. (ed.) (2021) *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*. Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html (Accessed: 29 January 2025).

Lange, R. (ed.) (2022) *Nastolatki wobec pornografii cyfrowej – Trajektorie użytkowania.* Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://cyberprofilaktyka.pl/badania/2022-nastolatki-a-pornografia-badania.pdf (Accessed: 29 January 2025).

Lange, R. (ed.) (2023) *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców.* Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://nask.pl/download-file/?fileId=15997 (Accessed: 29 January 2025).

Langevin, R., Curnoe, S. (2004) 'The use of pornography during the commission of sexual offenses', *International Journal of Offender Therapy and Comparative Criminology,* 48(5), pp. 572–586; https://doi.org/10.1177/0306624X03262518.

Lutkiewicz-Rucińska, A. (2023) 'Article 471' in Balwicka-Szczyrba, M., Sylwestrzak, A. (eds.) *Kodeks cywilny – Komentarz aktualizowany.*

Medycyna Praktyczna (2023) 'Rośnie liczba prób samobójczych dzieci i młodzieży', *mppl,* 30 August [Online]. Available at: https://www.mp.pl/pacjent/psychiatria/aktualnosci/330168,rosnie-liczba-prob-samobojczych-dzieci-i-mlodziezy (Accessed: 29 January 2025).

Ombudsman for Children (2023) *Rzecznik Praw Dziecka – Raport z badania: Dziennik codziennej aktywności dzieci i młodzieży.* Warszawa: Rzecznik Praw Dziecka [Online]. Available at: https://brpd.gov.pl/2023/04/28/badanie-codziennej-aktywnosci-mlodych-internet-a-potem-dlugo-dlugo-nic/ (Accessed: 29 January 2025).

Osiak, K. (2016) 'Prawa i obowiązki małoletniego pokrzywdzonego, które przysługują mu podczas przesłuchania w trybie art. 185a', *Kodeksu postępowania karnego: Dziecko Krzywdzone. Teoria Badania Praktyka,* 15(4), pp. 87–104 [Online]. Available at: https://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/613 (Accessed: 29 January 2025).

Piechna, J. (2020) *Szkodliwe treści w internecie. Nie akceptuję, reaguję! – Poradnik dla rodziców*. Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://www.gov.pl/web/niezagubdzieckawsieci/szkodliwe-tresci-w-internecie-nie-akceptuje-reaguje2 (Accessed: 29 January 2025).

Prokuratura Krajowa (2023) 'Kolejne uderzenie w przestępczość o podłożu pedofilskim w sieci', *gov.pl,* 3 November [Online]. Available at: https://www.gov.pl/web/prokuratura-krajowa/kolejne-uderzenie-w-przestepczosc-o-podlozu-pedofilskim-w-sieci (Accessed: 29 January 2025).

Prusak-Górniak, K., Silicki, K. (2019) 'Komentarz do Art. 26' in Czaplicki, K., Gryszczyńska, A., Szpor, G. (eds.) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz.* Warsaw: Wolters Kluwer.

Przemysław, N. (2024) 'Prokuratorzy z całej Polski wzięli udział w operacji „Enola Gay" wymierzonej w przestępczość o charakterze pedofilskim', *gov.pl,* 7 November [Online]. Available at: https://www.gov.pl/web/prokuratura-krajowa/prokuratorzy-z-calej-polski-wzieli-udzial-w-operacji-enola-gay-wymierzonej-w-przestepczosc-o-charakterze-pedofilskim https://www.gov.pl/web/niezagubdzieckawsieci/szkodliwe-tresci-w-internecie-nie-akceptuje-reaguje2(Accessed: 29 January 2025).

Sántha, F. (2024) 'Definition and Systematisation of Cybercrimes' in Gryszczyńska, A. (ed.) *Cybercrime*. Warsaw: Instytutu Wymiaru Sprawiedliwości, pp. 27–44 [Online]. Available at: https://wydawnictwo.iws.gov.pl/wp-content/uploads/2024/12/GRYSZCZYNSKA-Cybercrime_www.pdf (Accessed: 29 January 2025).

Staciwa, K. (2023) *Wykorzystywanie seksualne dzieci w cyberprzestrzeni: Analiza akt postępowań karnych ze szczególnym uwzględnieniem roli biegłych powoływanych w tych postępowaniach – Część I – teoretyczna.* Warsaw: Instytut Wymiaru Sprawiedliwości [Online]. Available at: https://dyzurnet.pl/publikacje (Accessed: 29 January 2025).

UKE (2021) 'Badanie konsumenckie dzieci i rodziców oraz nauczycieli 2020', *UKE,* 2 February [Online]. Available at: https://uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html (Accessed: 29 January 2025).

United Nations (1989) Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 [Online]. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (Accessed: 29 January 2025).

United Nations (2024) 'Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, adopted by the General Assembly of the United Nations on 24 December 2024 in New York by resolution 79/243' [Online]. Available at: https://docs.un.org/en/A/RES/79/243 (Accessed: 29 January 2025).

Vuorikari, R., Kluzer, S., Punie, Y. (2022) *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes.* Luxembourg: Publications Office of the European Union; https://doi.org/10.2760/115376.

Witkowska, M. (2020) *FOMO i nadużywanie nowych technologii.* Warsaw: NASK Państwowy Instytut Badawczy [Online]. Available at: https://www.gov.pl/web/niezagubdzieckawsieci/fomo-i-naduzywanie-nowych-technologii (Accessed: 29 January 2025).