

## CHILDREN’S RIGHTS IN THE DIGITAL ENVIRONMENT UNDER THE CONVENTION ON THE RIGHTS OF THE CHILD

Dr. Dawid Stadniczeńko

University of Economics and Humanities in Warsaw, Poland  
e-mail: [d.stadniczenko@vizja.pl](mailto:d.stadniczenko@vizja.pl); <https://orcid.org/0000-0001-6826-3366>

**Abstract.** The aim of this paper is to explain, based on the 1989 Convention on the Rights of the Child and its General Comment No. 25, how States Parties should implement the Convention in relation to the digital environment and provide guidance on appropriate legal, policy and other measures to ensure full compliance with their obligations under the Convention and its Optional Protocols in view of the opportunities, threats and challenges of promoting, respecting, protecting and fulfilling all children’s rights in the virtual environment. The author points out the current main threats in the execution of children’s rights in the digital environment and the challenges faced in this regard by the state authority, governmental and non-governmental organizations and the private sector.

**Keywords:** child; rights; cyberspace; digital environment; Convention on the Rights of the Child; danger

### INTRODUCTION

The number of sources of threats to children’s rights from cyberspace is labile. The emergence of drastically fast successive threats or evolving from the existing ones results in an increasing effort to make the public aware of them. This is particularly evident in the youngest generations, who by virtue of their “primordial” trust, so to speak, become easy victims of abuse by other users of the digital environment, and because of the lack of a real possibility for parents or legal guardians to control the successively emerging threats on the Internet, of which not only the quantity, but also their global content can be a major problem in the context of effective protection of children’s rights. The proliferation of online social platforms, applications, websites, transferring more and more matters of previous offline life to online life without introducing legal regulations, is very likely to lead to problems with the proper understanding of the nature of threats and the subsequent legal regulation of cyberspace, respecting human rights, especially children’s rights, and limiting the main types of threats. On the other hand, it should be kept in mind that even the best law cannot protect a person

from the threat of another person in the real world, or in cyberspace, when one is not aware of the dangers of individual-initiated actions in the process of globalization and the technological revolution. All authorities of the State Parties under the United Nations Convention on the Rights of the Child of November 20, 1989,<sup>1</sup> are obliged to take measures aimed at making the law a good and effective tool to combat such threats, but they are limited only to enacting increasingly harsh criminal laws [Broniatowski 2017]. Virtual violence, on the other hand, has become a much more difficult phenomenon to trace than real-world violence.

Given the above and the need to take into account that digital reality becomes the main reality in most aspects of children's lives (education, services, commerce, etc.) this has provided new opportunities to exercise children's rights, but also created the risk of their violation or abuse. The United Nations Committee on the Rights of the Child<sup>2</sup> drafted General Comment No. 25<sup>3</sup> to the United Nations Convention on the Rights of the Child of November 20, 1989, addressing the challenges as well as the risks based on consultations with both children and experts, reports from States Parties, jurisprudence of human rights treaty bodies, recommendations of the Human Rights Council, to provide States Parties to the Convention with a tool to properly understand its provisions in a world that is changing around us.<sup>4</sup>

The aim of this paper is to explain, based on the Convention on the Rights of the Child and its General Comment, how States Parties should implement the aforementioned Convention in relation to the digital environment and provide guidance on appropriate legal, policy and other measures to ensure full compliance with their obligations under the Convention and its Optional Protocols in view of the opportunities, threats and challenges of promoting, respecting, protecting and fulfilling all children's rights in the virtual environment.<sup>5</sup> The paper uses the method of document research as well as analysis and literature criticism (sources). A scientific research technique in the form of observation and document study was also used.

## 1. CYBERSPACE AND THREATS

Cyberspace is defined in the subject literature as all links of a virtual nature ("non-spatial" in the physical, intangible and geographical sense),

---

<sup>1</sup> Convention on the Rights of the Child of 20 November 1989, Journal of Laws of 1991, No. 120, item 526 [hereinafter: Convention].

<sup>2</sup> Hereinafter: CRC.

<sup>3</sup> General comment No. 25 (2021) on children's rights in relation to the digital environment, Committee on the Rights of the Child, CRC/C/GC/25, United Nations, March 2, 2021.

<sup>4</sup> *Ibid.*, p. 1-2.

<sup>5</sup> *Ibid.*, p. 2.

which were created and function thanks to their physical guarantors (computers, telecommunications infrastructure) [Madej 2009, 28]. In summary, it can be stated that cyberspace represents "all of the interrelationships of human activity involving ICT (Information and Communication Technology)" [Bógdał-Brzezińska and Gawrycki 2003, 37].

Referring to the definition of a child, the one expressed in Article 1 of the 1989 Convention on the Rights of the Child, which stipulates that a child is a human being before the age of 18, unless he or she attains majority earlier in accordance with the law relating to the child, should be considered the most universal. The Convention, by virtue of the fact that the date of its enactment is 1989, does not contain provisions that directly refer to the protection of children from the threats of cyberspace, which is obviously due to the fact that the Internet and the virtual world were not yet as developed and widely available as they are today.

Threats that are currently identified in various aspects are: infoholism/dataholism, cyberholism, video game addiction, computer addiction, FOMO (Fear of Missing out) and others. Being "logged" into the digital world all the time, as well as its sudden withdrawal, also impinges on the mental and physical spheres, which is expressed in feelings of loneliness, psychomotor restlessness, experiencing fear, nausea, dizziness, abdominal pains and general discomfort, which may cause identity disruption of the growing child in the future. On the other hand, children, even more so in infancy, pre-school age tend to become victims of their own parents' activities (sharenting), which involves regularly posting detailed information (photos, videos and other content) about their children on social media. Sharenting should be distinguished from the activity of parents called troll parenting, which means sharing content that directly embarrasses or shames children or shows difficult moments for them [Chrostowska 2018, 59]. It is also important not to forget the long-standing problem of creating, storing and sharing child pornography, the underlying nature of which has changed significantly with the development and use of ICT [Eneman 2004, 29]. Despite the existence of several momentous international legal acts mainly of a European nature,<sup>6</sup> it is their provisions that are, in principle, directed to protect children from exploitation by adults (as well as numerous public and private entities), leaving individual states freedom to regulate any sexual activities

---

<sup>6</sup> These include the following legal acts: Lanzarote Convention of the Council of Europe of 25 October 2007 on the Protection of Children against Sexual Exploitation and Sexual Abuse (Journal of Laws of 2015, item 608); 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, replacing Council Framework Decision 2004/68/JHA (OJ EU.L.2011.335.1 of December 17, 2011); Council of Europe Convention on Cybercrime, drawn up in Budapest on 23 November 2001 (Journal of Laws of 2015, item 728).

between minors if they are undertaken with their mutual consent, or specify what activities related to new technologies and the development of information systems its signatories are to criminalize in their legal systems. However, these are not sufficient dispositions in such a sensitive social group as children, especially taking into account the incredibly dynamic area that is the digital environment.

## 2. GENERAL PRINCIPLES OF THE CONVENTION ON THE RIGHTS OF THE CHILD IN RELATION TO THE DIGITAL ENVIRONMENT

From a socio-legal point of view, it is a truism nowadays to say that the rights of every child must be respected, protected and exercised in every corner of the world. The same applies in the digital environment as well, especially as cyberspace can be an instrument to help violate human rights [Schutlz 2008, 94]. Innovations in digital technologies affect children's lives and their rights in broad and interdependent ways, even if children themselves have no or limited access to the Internet. Significant access to digital technologies can support children in exercising the full range of their civil, political, cultural, economic and social rights.

The Convention, being the main international legal regulation on the safety of children and adolescents in the digital environment, despite its nature as a legal act having worldwide application in very different social, economic and political conditions, is a very important tool for the protection of children's rights, defining these rights and instructing States Parties to take multifaceted measures aimed at implementing the realization of these rights. It contains general provisions (see, e.g., Articles 19 and 34) that provide a legal basis for the introduction of regulations in national legal systems related to the protection of children and adolescents in cyberspace.

In order to facilitate a proper understanding and identification of the measures needed to guarantee the exercise of children's rights in relation to the digital environment, attention should be paid to the four basic general principles expressed in the Convention, i.e., the principle of non-discrimination (Article 2), the principle of the best interests of the child (Article 3), the right to life, survival and development of the child (Article 6), and respect for the views expressed by the child (Article 12).

The principle of non-discrimination under General Comment No. 25 resonates in that children can be discriminated against being excluded from the use of digital technologies and services – 1.3 million children do not have access to the Internet [Mizunoya, Avanesian, et al. 2020] – or receiving hateful messages or unfair treatment as a result of using these technologies. Other forms of discrimination can occur when automated processes that

result in information filtering and collection, profiling or decision-making are based on biased, partial or unfairly obtained data about a child. An important non-discriminatory factor to implement is overcoming digital exclusion among children, which includes providing free and safe access for children in designated public places and investing in policies and programs that support affordable digital access and knowledge-based use for all children in educational institutions, communities and homes.

The principle of the best interests of the child, as a dynamic concept expressed in the Convention in the context of children's rights protection in cyberspace, imposes on States Parties that the best interests of every child are to be prioritized in all activities concerning the provision, regulation, design, management and use of the digital environment involving national and local authorities overseeing the execution of children's rights in such activities.

The right to life, survival and development involves risks associated with the conduct of users online or with the content provided, which include, but are not limited to, such as violent and sexual content, cyberbullying, gambling, and various types of exploitation and abuse, including sexual exploitation and abuse, and the promotion or incitement of suicide or life-threatening activities, including by criminals or terrorist/extremist groups. States Parties and their appointed authorities should identify and respond to emerging threats faced by children in various contexts. The Committee emphasizes that the use of digital devices should not replace personal interactions between children or between children and parents or guardians. States Parties should pay particular attention to the effects of technology in the earliest years of life, when flexibility of the brain is at its maximum and the social environment, particularly relationships with parents and caregivers, is crucial in shaping children's cognitive, emotional and social development. Training and advice on the appropriate use of digital devices should be provided to parents, caregivers, teachers and other relevant actors, taking into account research on the impact of digital technologies on children's development, especially during the neurological growth spurts of early childhood and adolescence.

In the context of the last principle, i.e., respect for the child's views, which should be taken into account and viewed through its prism for the execution of all the children's rights contained in the Convention regarding the digital environment, it should be pointed out that children have a positive perception of the virtual world, as it provides them with opportunities to have their voices heard on issues that affect them, which undoubtedly helps children's participation in initiatives at various levels, from local to international. In this regard, the Committee indicates that States Parties should already involve children in legislative work, listen to their needs and give

due weight to their views (according to the maturity they present). However, it is not only public authorities that have a role to play in respecting children's views, as digital service providers should also actively cooperate with children, using appropriate protections, and giving due consideration to the views of underage users when developing products and services. It should be noted that the digital environment is the most accessible environment to connect people in a timely manner and convey necessary information.

The use of the digital environment should also be in the field of activating minors in cooperation with civil society, which is undoubtedly a major challenge for both the public and private sectors that should systematically involve children in cooperation with civil society, through education, development, implementation, monitoring and evaluation of laws, policies, creation of plans and programs adapted to the different developmental phases of the child regarding the deepening of children's rights awareness.<sup>7</sup>

### 3. DIGITAL ENVIRONMENT AND SELECTED CIVIL RIGHTS AND FREEDOMS

Digital Human Rights (DHR), is now an extension of basic human rights to secure digital data linked to a person's identity and behavior in the physical or virtual realm. Digital data is a multifaceted tool, with enormous political and economic power. For state actors, cyberspace and digital data are used as a tool that provides a way to guarantee public safety and protect national security interests. For human rights advocates, digital data is inextricably linked to personal identity. It should be protected as a fundamental human right by all who produce, store and use it [Dowd 2022, 249].

A key aspect of effective Internet and digital safety involves beginning education (primarily learning to read) in this area in the early years, as safety can be related to the level of understanding the Internet among young children according to their social and cultural context. In particular, this refers to research suggesting that older children adapt the Internet to the perceptual dimensions of the technologies they use when participating in a variety of online activities [Edwards, Skouteris, et al. 2016, 43].

The proper exercise of children's rights and their protection in the digital environment requires a wide range of both legislative, administrative and preventive measures. For this purpose, the Committee points out that they should be updated on an ongoing basis so that legislation remains up-to-date in the context of technological advances as well as emerging practices and potential risks.<sup>8</sup> On the other hand, any legislative measures must be

---

<sup>7</sup> General comment No. 25 (2021) on children's rights..., p. 7.

<sup>8</sup> *Ibid.*, p. 8.

complemented by permanent education of skillful and safe use of cyberspace, as without education, it seems, it will not be possible to ensure children's safety in cyberspace [Sitek and Such-Pyrgiel 2019, 212].

The digital environment also provides children with an unprecedented opportunity in the history of the world to exercise their right of access to information (Articles 13 and 17 of the Convention) through information and communication media. In doing so, States Parties should ensure that children have access to information in this digital environment and that the exercise of this right is limited only when provided for by law and necessary for the purposes set forth in Article 13(2) of the Convention, which states that the exercise of this right may be subject to certain limitations, but only those that are provided for by law and that are necessary: (1) to respect the rights or reputation of others; or (2) to protect national security or public order, or public health or morals. The Comment also points out to digital service providers, on their initiative, to take steps for the use of concise and understandable labeling of content potentially directed at children, for example, in terms of age appropriateness or content credibility emphasizing that content moderation and control should be balanced with the right to be protected from violations of children's other rights, in particular their rights to freedom of expression and privacy.

States Parties should respect the child's right to freedom of thought, conscience and religion in the digital environment in accordance with Article 14 expressed in the Convention. An important requirement of the Committee is to introduce or update (depending on the state of legislation in a given country) data protection laws and standards that identify, define and prohibit practices to manipulate or interfere with children's right to freedom of thought and belief in the digital environment, for example, through emotion analysis or inference. It should be noted that it is already possible to draw conclusions about a child's mental state using artificial intelligence. They should ensure that these automated systems or information filtering systems are not used to influence children's behavior or emotions leading to a limitation of their capabilities or proper development. Access to the Internet is, of course, access to information, regardless of what people think about the content (good or bad). To prohibit this access is to deny every citizen the opportunity to exercise their right to express themselves [Guinchard 2010, 8].

The Committee also emphasized that the digital environment and what it offers can enable children to shape their identities in many ways and participate in connected communities and public spaces for debate, cultural exchange, social cohesion and diversity, while realizing freedom of association and peaceful assembly in the digital environment. At the same time, it pointed out the undoubtedly positive aspect that "public visibility" and

networking opportunities in the digital environment can also support and create activism for underprivileged children, socially and enabling them to communicate freely with each other, defend their rights and form associations, thus making them human rights defenders.<sup>9</sup>

Another right relevant to the digital environment is the right to privacy (Article 16 of the Convention). The processing of children's personal data is usually motivated by offering educational and health benefits. However, some data may contain information on children's identity, activities, location, communication, emotions, health and relationships, among others. Some combinations of this personal data, including the increasingly popular biometric data, can uniquely identify a child, which directly violates the right to privacy, especially if identity theft occurs as a result of inadequate security. Threats can also come from children's own actions and those of family members, peers or others, such as by parents sharing photos online or strangers sharing information about a child. On the other hand, the protection of a child's privacy in the digital environment may be inadequate when parents or legal guardians pose a threat to the child's cybersecurity, which happens very often when they are in conflict, such as in determining custody of the child. In this aspect, reasonable control of data by the child's legal and actual guardians is of great importance. As the Committee highlights, interference with a child's privacy is permissible only if it is not arbitrary or unlawful. Therefore, any such interference should be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed with the best interests of the child in mind, and must not interfere with the laws, purposes or objectives of the Convention.<sup>10</sup> Electronic surveillance currently practiced by most countries around the world violates an individual's right to privacy, a fundamental right enshrined in Article 17 of the International Covenant on Civil and Political Rights. In many cases, electronic surveillance is a prelude to censorship. State censorship, which includes suppression of banned content and possible sanctions against the user, is the next step in the chain of digital surveillance. Censorship can violate an individual's right to freedom of thought, expression and association, but like privacy, it can be suspended to "protect public safety, order, health or public morals, or the fundamental rights and freedoms of others"<sup>11</sup> [Perry and Roda 2017, 64-65].

---

<sup>9</sup> Ibid., p. 12.

<sup>10</sup> Ibid., p. 13.

<sup>11</sup> International Covenant on Civil and Political Rights opened for signature in New York on 16 December 1966 (Journal of Laws 1977, No. 38, item 167).



## CONCLUSIONS

It is necessary to be aware that there are always two sides to every coin – along with the benefits of the Internet and other digital tools, there are also new and evolving threats, such as exposure to inappropriate content, vulnerability to offline violence, concerns about overuse and time-killing, as well as countless data protection and privacy issues. As recent advances in technical and non-technical fields have made it really difficult to draw a contrast between the online and offline worlds, it has become increasingly necessary to analyze how this drastic change affects children's well-being, development and rights<sup>12</sup> [Sahoo 2016, 37]. Some countries and governing entities have been implementing general regulatory measures to address individual data privacy management, data collection and analytical practices, but these measures are partial, adapted to current technical capabilities, and do not take into account the techniques and learning capabilities of artificial intelligence and intelligent data collection, the potential framework of which has not been determined. Until then, it is crucial to raise the issues about the functioning of effective child protection in the digital environment [Willson 2021, 323].

One of the most important measures that need to be taken to exercise children's rights in the digital environment is the issue of orderly and clear collection of personal information/data that anyone, at any time, will be able to review and possibly refuse to disclose to specific entities. This is one of the main challenges in actively protecting children's rights in a properly managed digital environment.<sup>13</sup>

Taking Poland as an example, it is possible to note that the legal regulations in Poland relating to the safety of children and adolescents in cyberspace, indicate a clear predominance of provisions of a criminal law nature, which means that the role of the law mainly comes down to the imposition of sanctions, determining what actions will be prosecuted and punished by the justice system while pursuing the well-known functions of criminal law, which are the protective, guarantee and compensation functions [Giezek 2020, 30-33]. On the other hand, the problem of punishment of minors arises. In the science of law, for example, there is an ongoing dispute over the permissibility of the non-statutory counter-type of "chastisement of minors," if it serves an educational purpose and is intended to protect the welfare of the child [Jedlecka 2020, 97].

As has been pointed out, even the best provisions of criminal law, by itself, are not able to ensure that such acts are not committed. Thus, it would

---

<sup>12</sup> See Claude and Hick 2000, 231; Schutlz 2008, 94-97 and the literature cited there.

<sup>13</sup> General comment No. 25 (2021) on children's rights..., p. 12-13.

be naive to believe that even the best laws, will be able to protect children and adolescents from the threats of cyberspace. All States Parties under the Convention on the Rights of the Child are obliged to take steps aimed at making the law a good and effective tool to combat such dangers, but not heading towards enacting ever harsher criminal laws, rather than educating both parents, caregivers and minors from their earliest years of life [Broniatowski 2017; Mackintosh 2019; Claude and Hick 2000, 231; Schutlz 2008, 94-97]. On the other hand, the increasingly emerging restrictions on freedom of expression in cyberspace focus on blocking access instead of creating and moderating expression. This raises the debate on human rights, including children's rights to access expression.

#### REFERENCES

- Bógdał-Brzezińska, Agnieszka, and Marcin Gawrycki. 2003. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. Warszawa: Oficyna Wydawnicza ASPRA-JR.
- Broniatowski, Krzysztof. 2017. "Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni – regulacje w prawie polskim i unijnym." Warszawa: Kancelaria Sejmu. Biuro spraw senatorskich. [https://www.senat.gov.pl/gfx/senat/userfiles/\\_public/bss/dokumenty/new/171002/bezpieczenstwo\\_dzieci\\_i\\_mlodziemy\\_wersja\\_ostateczna.pdf](https://www.senat.gov.pl/gfx/senat/userfiles/_public/bss/dokumenty/new/171002/bezpieczenstwo_dzieci_i_mlodziemy_wersja_ostateczna.pdf) [accessed:14.09.2022].
- Chrostowska, Bożena. 2018. "Sharenting – skala i wielowymiarowość zjawiska (nierozważnego) ujawniania przez rodziców informacji o dzieciach w mediach społecznościowych." *Problemy Wczesnej Edukacji* 4, no. 43:58-68.
- Claude, Pierre R., and Steven Hick. 2000. "Human Rights Education on the Internet: Its Day Has Come." In *Human Rights and the Internet*, edited by Steven Hick, Edward Halpin, and Eric Hoskin, 225-37. London: Palgrave Macmillan.
- Dowd, Rebekah. 2022. *The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU*. Switzerland: Palgrave Macmillan.
- Edwards, Susan, Helen Skouteris, et al. 2016. "Young children's internet cognition." In *Understanding digital technologies and young children. An international perspective*, edited by Susanne Garvis, and Narelle Lemon, 38-45. New York: Routledge.
- Eneman, Marie. 2004. "The New Face of Child Pornography." In *Human rights in the digital age*, edited by Andrew Murray, and Mathias Klang, 27-40. London: Routledge.
- Giezek, Jacek. 2020. "Pojęcie i funkcje prawa karnego." In *Prawo karne materialne. Część ogólna i szczególna*, edited by Marek Bojarski, 30-33. Warszawa: Wolters Kluwer.
- Guinchard, Audrey. 2010. "Human Rights in Cyberspace." *Society of Legal Scholars Conference (SLS)*. SSRN Electronic Journal. 1-13. Doi: 10.2139/ssrn.1694483
- Jedlecka, Wioletta. 2020. "Zakaz stosowania kar cielesnych a kontratyp karcenia wychowawczego." *Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji* CXX/2, no. 3978:97-108. DOI: 10.19195/0137-1134.120.55

- Mackintosh, Eliza. 2019. "Special Report. Finland is winning the war on fake news. What it's learned may be crucial to Western democracy." Atlanta: CNN. <https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/> [accessed: 11.09.2022].
- Madej, Marek. 2009. "Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego." In *Bezpieczeństwo teleinformatyczne państwa*, edited by Marek Madej, and Marcin Terlikowski, 17-40. Warszawa: Polski Instytut Spraw Międzynarodowych.
- Mizunoya, Suguru, Garen Avanesian, et al. 2020. "How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic." New York: UNICEF. <https://data.unicef.org/resources/children-and-young-people-internet-access-at-home-during-covid19/> [accessed: 14.09.2022].
- Perry, Susan, and Claudia Roda. 2017. *Human Rights and Digital Technology*. London: Palgrave Macmillan
- Sahoo, Anshuman. 2016. "Children's rights in the cyberspace." *International Journal of Research and Analysis* 4, issue 2:36-45.
- Schultz, William. 2008. "Human Rights and Cyberspace." *New Perspectives Quarterly* 19, no. 2:94-97. Doi: 10.1111/0893-7850.00509
- Sitek, Magdalena, and Małgorzata Such-Pyrgiel. 2019. "Influence of cyberculture on human rights." *Journal of Modern Science* 39(4):201-15. Doi:10.13166/jms/101510
- Willson, Michele. 2021. "Digital Predictions: Children's Futures, Opportunities and Obstacles." In *Young Children's Rights in a Digital World. Play, Design and Practice. Children's Well-Being: Indicators and Research Volume 23*, edited by Donell Holloway, Michele Willson, Karen Murcia, et al. 313-26. Switzerland: Springer.