| Chapter 5 |

Children in Digital Age – European Union and Central European Best Practices and Challenges

Katalin Baracsi

ABSTRACT

This chapter delves into the crucial issue of child protection in the digital age, examining the landscape in both the European Union and Central European regions. The narrative unfolds through the lens of the author's 16-year experience conducting interactive sessions on safe internet use for various age groups. Despite the pervasive influence of technology, some individuals resist internet adoption, even for their children. Moreover, the chapter underscores the dual nature of the Internet, presenting both opportunities for legitimate users and risks from criminal activities. The primary focus of the chapter is to scrutinise existing child protection legislation, institutions, and authorities in the context of online safety. The analysis employs a blend of theoretical and practical approaches, utilising a diverse range of sources, particularly from the online realm. The chapter explores gaps in the legal framework and institutional background, aiming to identify areas for improvement.

KEYWORDS

child online protection, online risks, digital media literacy, cybersecurity, children and youth safety

1. Introductory Ideas

'You can live without the Internet, but it's not worth it', a Danish lady in Elsinore, preparing to celebrate her eightieth birthday, told me a few years ago. Every week, she meets friends and strangers from the area to learn about safe and aware internet use at the local, technically equipped old people's club. For 15 years I have been running interactive sessions on safe internet use for children, young people, interested adults, and professionals. Occasionally, but there are still some participants who say they do not use the Internet, even hate it, and do their best to give their children access to the web as late as possible. In such cases, I use the example of the Danish lady and point out to the doubters that this may not be their world, but it is the present and the future for the generation now growing up. If we deprive them of this knowledge, we will be putting them at a disadvantage in the real world, which will be fraught with failure

Katalin Baracsi (2025) 'Children in Digital Age – European Union and Central European Best Practices and Challenges' in Halász, Cs. (ed.) (2025) *Children in Digital Age.* Miskolc–Budapest: Central European Academic Publishing, pp. 87–103. https://doi.org/10.71009/2025.csh.cida_5.

for them. Nor must we forget that rapid technological progress and the unlimited possibilities of the Internet offer new opportunities not only for bona fide users but also for criminals. Crimes can and are being committed online. Parents, educators, and all of us have a shared responsibility to prepare them for this brave new world and to protect them from the risks and dangers they face online.

In this chapter I examine how existing child protection legislation, institutions, and authorities support and promote child online protection, what is missing in the legal framework and institutional background, and where and how it can be improved. I will apply both theoretical and practical approaches. Because of the nature of the topic, the sources used will include a greater number of writings from the online world. In addition to exploring the legal context, I will also pay particular attention to the objectives to be achieved in the future in the Czech Republic, Hungary, Poland, and the Slovak Republic.

2. Digital Intelligence (DQ), the New Superpower

I first encountered the concept of digital intelligence in a blog post by Bertalan Péter Farkas in 2016.[1] It is a set of social, emotional, and cognitive skills that are indispensable for digital life. Knowledge, skills, and abilities to perceive and adapt to the feelings of others or regulate the behaviour of others to cope with the challenges and needs of the digital space.

The term is not yet part of our everyday communication, but I think it is something that has existed since the advent of the Internet; we are just now getting around to giving it a summary name and starting to look at the skills and competences we need to make conscious and responsible use of the opportunities offered by the online space.

Digital intelligence, according to the model, can be divided into eight skill sets:

1. *Digital identity:* skills for creating and managing online identity and reputation. This includes an individual's online presence and the ability to manage their online presence and behaviour in the short and long term.
2. *Digital balance*: the controlled use of digital tools and media to achieve a healthy balance between offline and online life.
3. *Digital confidence:* the ability to manage online risks (cyberbullying, radicalisation) and problematic content online, including the ability to avoid and control them.
4. *Digital security:* the ability to detect cyber threats (hacking, online fraud, phishing, malware attacks) and find appropriate and appropriate ways to protect your data.
5. *Digital emotional intelligence:* the ability to empathise and build good online relationships.

1 Farkas, 2016.

6. *Digital communication:* the ability to communicate and collaborate with others using technology and media.
7. *Digital literacy:* a set of skills that enable the discovery, evaluation, and use of appropriate content using algorithmic thinking.
8. *Digital rights*: the ability to understand and support personal and legal rights, including the right to privacy, protection of intellectual property, freedom of expression, and protection against hate speech.

It is not by chance that I wanted to refer to this model, as digital rights are included as a stand-alone issue, which further reinforces the need to create a legal environment that is safe for all as an essential pillar of online child protection. Research on the Digital Intelligence project[2] is currently at the stage where researchers are working on the development of a test battery that will measure digital intelligence (DQ) after intelligence (IQ) and emotional intelligence (EQ). I look forward to seeing when they will be ready and how digital literacy will be measured.

3. What Is Child Online Protection and Why Do We Need It?

Child online protection is a set of different approaches to reduce the risks and dangers children face in online spaces. All adults have a shared responsibility to protect children from these dangers.[3] Children and young people are the primary targets of online child protection, but to keep them safe, it is essential to have the help and support of the adults around them. Knowledge transfer, empowerment, and an appropriate legal and technical environment are all part of child online protection. In many cases, when we are doing something – buying an internet subscription for our child's mobile phone – we do not even realise that we are exercising our right to access the Internet, which is also part of child online protection. To understand this area better, it is worth reviewing the current state of the Internet and dispelling some misconceptions.

3.1. Internet Usage and Users Today[4]

According to International Telecommunication Union (ITU) data, there were an estimated 4.1 billion people using the Internet in 2019, reflecting a 5.3 per cent increase compared to 2018 estimates.

Children and young people use the Internet for a variety of purposes, from getting information for a school project to chatting with a friend. They are highly proficient in mastering complex programs and applications, connecting to the Internet using

2 See: https://www.dqinstitute.org/ (Accessed: 10 January 2024).
3 International Telecommunication Union, 2020a, p. 6.
4 International Telecommunication Union, 2020b, pp. 1–5.

mobile phones, tablets, and other handheld devices such as watches, iPod Touches, e-book readers, and gaming consoles.[5]

The Internet has also acted as an important tool in the lives of the different groups of children and young people with vulnerabilities. For migrant children, it maintains a connection with family and friends and offers a window into the culture of their new home. It enables children and young people with disabilities to socialise and to be involved in activities that are unavailable offline and provides opportunities to be on an equal footing with peers online, with abilities more visible than disabilities.

However, the Internet, along with providing access and opportunities, also provides risk and harm, with some more prone than others. For instance, for migrant children and young people, the consequences of an online breach of confidential information could be dramatic – in the wrong hands, data could be used to identify and target people based on their ethnicity, immigration status, or other identity signifier;[6] for children and young people with autism spectrum disorder (ASD), social challenges such as difficulty in understanding others' intentions can leave this group vulnerable to "friends" with bad intentions; and children and young people with disabilities are more prone to exclusion, stigmatisation, and manipulation.

Many parents and guardians are under a common misconception that their child is safer if they use the computer at home or at school than elsewhere. This is a dangerous misconception because the Internet can take children and young people virtually anywhere in the world, and in the process, they can be exposed to potentially dangerous risks, just as they could in the physical world. However, children and young people do experience slightly increased risk of harm when accessing the Internet via a smartphone, tablet, or other handheld devices. This is because these handheld devices give instant access to the Internet from anywhere and are less likely to be monitored by parents or carers.

These guidelines have been developed within the child online protection initiative, as part of the ITU Global Cybersecurity Agenda,[7] with the aim of establishing the foundations for a safe and secure cyberworld not only for today's youth but also for future generations. These guidelines also focus on children with vulnerabilities, particularly migrant children, children with ASD, and children with disabilities.

At the global level, one in three Internet users is under 18,[8] a staggering amount given that in 2018, more than half of the world's population used the Internet. In developing countries, children are leading Internet use, growing up with the Internet, and connecting with mobiles first.[9]

With more children around the world gaining access, the fulfilment of their rights will increasingly be shaped by what happens online. Internet access is fundamental

5 International Telecommunication Union, 2019.
6 UNICEF, 2017.
7 International Telecommunication Union, 2020c.
8 Livingstone, Carr and Byrne, 2015.
9 International Telecommunication Union, 2020d.

to the realisation of children's rights. With one child in three being an Internet user, there are still about 346 million children worldwide that are not connected.[10]

Those who could most especially benefit from the opportunities the Internet offers are often the least connected. We see that in the Africa region around 60 per cent of children are not online, compared to 4 per cent in Europe.[11]

In terms of access to the Internet, there are also significant differences by gender. Research[12] shows that in every region except the Americas, male Internet users outnumber female users. In many countries, girls do not have the same access opportunities as boys, and even where they do, girls are often monitored and restricted in their internet use to a much greater extent.

Digital divides go beyond the question of access. Children who rely on mobile phones rather than computers may get only a second-best online experience, and those who lack digital skills or speak minority languages often cannot find relevant content online. Children from rural areas are more likely to experience theft of passwords or money. They also tend to have lower digital skills, spend more time online (especially playing games), and receive less parental mediation and monitoring.[13]

Both children and adults report that the digital divide is an ongoing concern and requires dedicated investment and creative solutions. Children in these settings are coming online in ever greater numbers, but many do not benefit from appropriate forms of guidance from parents, teachers, and other significant adults. This continues to place children at risk.

The Internet has become a tremendously enriching and empowering technology. Children and young people have been major beneficiaries of the Internet and related digital technologies. These technologies are transforming the way we all communicate with each other and have opened many new ways to play games, enjoy music, and engage in a vast array of cultural activities and participation, dissolving many barriers. Children can broaden their horizons online by taking advantage of opportunities to gather information and nurture relationships. The Internet provides access to health, educational services, and information on topics that are important for young people but may be taboo in their societies. Children and young people have very often been at the forefront of adopting and adapting to the possibilities provided by the Internet.

Yet, it is undeniable that the Internet has brought in its wake a range of challenges to children's and young people's safety, which need to be addressed, both because they are important and also because it is important to communicate to everyone concerned that the Internet is a medium that can be trusted. Equally, it is essential that the concern to protect children and young people online is not allowed to become

10 UNICEF, 2017.
11 Ibid.
12 Sey and Hafkin, 2019.
13 UNICEF, 2019

a platform to justify an assault on free speech, free expression, or the freedom of association.

It is extremely important for the next generation to feel confident about using the Internet so that they can, in turn, continue to benefit from its development. Thus, when discussing the safety of children and young people online, it is vital to strike the right balance.

It is essential to discuss openly the risks that exist for children and young people online, to teach them how to recognise risk and prevent or deal with harm should it materialise, without unduly frightening or exaggerating the dangers.

Any approach that deals only or largely with the negative aspects of the technology is very unlikely to be taken seriously by children and young people. Parents and teachers can often find themselves at a disadvantage because young people will very often know more about the technology and its possibilities than older generations. Research has shown that most children are able to distinguish cyberbullying from joking or teasing online, recognising that cyberbullying is designed to harm. In many parts of the world, children indeed have a good understanding of some of the risks they face online.[14]

However, while it might be deduced that efforts to skill children to manage online risks are effective, there is still scope to raise the awareness of many more children around the world, particularly among vulnerable groups, and concerted efforts must focus on these children, especially to improve awareness of support services for victims of cyberbullying and other forms of online risks.

There are many challenges ahead. Not only does access to the connected world pose problems. The rate of technological change presents challenges for the safety of children online. Many children navigate a complex digital media landscape. Developments in artificial intelligence and machine learning, virtual and augmented reality, big data, facial recognition, robotics, and the Internet of Things are set to transform children's media practices even further.

It is critical that all stakeholders plan for and think through the consequences of these developments for children and find ways to support them to develop the necessary digital literacies not just to survive but to thrive in the digital future. Further investment in the digital skills and literacies of parents and teachers is required to support children to develop the critical thinking and evaluative skills to enable them to navigate fast-paced flows of information of varying quality and from parents and educators to children, to become digital citizens.[15]

14 Since 2016, ITU has undertaken consultations within COP with children and adult stakeholders on relevant issues such as cyberbullying, digital literacy, and children's activities online.
15 Council of Europe, 2016.

4. Strategic Context for Child Online Protection[16]

When developing international and national strategies for child online protection, policymakers and legislators need to take different aspects into account. They need to get to know and engage with the following individuals and organisations to understand their experiences, views, opinions, activities, and actions: children and young people; parents, carers, teachers; ministries; industry and related service providers; researchers and academics; NGOs; law enforcement agencies; health and social organisations.

Because so many people are involved, there are already measures in place to protect children in the online space, but they may work independently of each other. It is important to be aware of the mechanisms already in place before creating a national strategy. Align the objectives of the strategy with the measures already in place and add new points. The strategy should be integrated into existing frameworks or merged with similar strategies already in place.

In addition to understanding the actions and experiences of the different stakeholders, it is also important to consider national specificities and the actions of other countries. There have been innovative developments and initiatives in the regulatory and organisational responses to ensure children's online safety and well-being. It is important to assess the possibilities, but reviewing existing measures and options and working with other similar areas can also help policy makers and legislators.

The national child online protection strategy has benefits. Developing appropriate national legislation, creating the necessary legal framework, and harmonising it with international measures is a key step in protecting children online. These frameworks can be self-regulatory, co-regulatory, or fully regulated legal frameworks.

Once we are aware of existing national measures, options, and good practices and consider the examples of other countries and legislators, we can start developing our own national child online protection strategy.

4.1. The Framework of Child Online Protection

The framework should include all possible online threats to children and should not unduly restrict children's rights.

The new regulatory framework should fit in with existing regulations. The risks of online sexual exploitation of children (including the production of sexual content) and the national training opportunities for professionals should be clearly defined. It is important that the framework details the objectives and defines the evaluation criteria.

A strategy should be developed that reaches out to all stakeholders and is able to define, coordinate, and operate national actions as part of a national child online protection strategy. This mechanism should be a tool to bring together and guide

16 Based on Council of Europe, 2016; International Telecommunication Union, 2020a, pp. 7–10.

stakeholders across the country and make the day-to-day functioning of child online protection more effective. To fully implement a national child online protection strategy, a checklist should be created and filled in according to the following model.

Legal framework: Review existing legislation to help law enforcement agencies and other organisations protect under-18s online on accessible internet platforms. Once the relevant parts have been reviewed, make clear that any offence committed against children in the offline world is also a crime in the online space and ensure that children's online privacy is protected.

Regulatory framework: Regulatory developments should also be reconsidered. They can be self-regulation, co-regulation, or full regulation.

Reporting illegal content: Create a platform with easy-to-understand information to easily report illegal content found on the Internet. Advertise this service widely.

Reports: Industry players and representatives of the corporate sector should provide a way for users to report their problems and concerns about the online space and receive appropriate responses.

Sponsors: All stakeholders should be able to participate in online child protection.

Research: Conduct a survey of those working on the issue to gauge their views, needs, experiences, concerns, and opportunities in relation to online child protection.

Digital media literacy education: Include age-appropriate digital literacy education in school curricula.

Educational materials: Formulate messages and produce information materials related to internet safety that are in line with legal regulations. Distribute them to all stakeholders.

Child protection: Ensure that comprehensive child protection measures are in place to oblige all those who work with children to recognise, deal with, and report abuse and other online threats.

National awareness: Organise national educational campaigns to raise awareness of online child protection issues.

Tools, services, and settings: Consider the useful features of digital devices, technical tools (such as the filtering function), and child protection apps and settings that help you in your daily work.

5. The European Union and Child Online Protection

All four countries are members of the European Union, so the legislation they have in place in child online protection legislation also affects their digital daily lives. Almost at the same time as the Internet was expanding at an unstoppable pace, in the early 2000s the European Union recognised the need to develop measures to ensure the safety of the online world, which was becoming increasingly abusive as the number of Internet users grew. In practice, this means that each Member State is obliged

to set up a consortium of one or more people to promote safer internet use in their country.

5.1. Together for a Better Internet

The European Commission launched the Safer Internet Plus Programme in 2004. Its aim is to make the Internet and online technologies safer to use, especially for children, in line with the values promoted by the European Union, and to improve the effectiveness of the fight against illegal and harmful content.

These objectives can be achieved by the following means: hotlines to combat illegal and harmful content; helpline, e-mail, and chat consultation for children and young people who have encountered harmful, dangerous content or bullying on the Internet; raising awareness among users; measures to combat unwanted and harmful content (filtering systems, information exchange, child protection measures, closer police/criminal cooperation); promoting a safer environment (emphasis on self-regulation).[17]

The Safer Internet Programme[18] in 31 European countries (all four Central European countries presented) is a good basis for ensuring that child protection online works at the network level. It allows countries to build links and develop and exchange good practice, which contributes to keeping the digital child protection agenda active and continuously evolving. In addition to the Safer Internet consortia partnerships, which are largely run by NGOs, other EU efforts are worth mentioning. Joint European action can help to unify key aspects of online child protection across borders and enhance international cooperation and action on a Europe-wide basis.

The Digital Agenda for Europe aims to have every European digital. Children have particular needs and vulnerabilities on the Internet; however, the Internet also provides a place of opportunities for children to access knowledge, to communicate, to develop their skills, and to improve their job perspectives and employability.

The original "Strategy for a Better Internet for Children", published in 2012, proposed a series of actions to be undertaken by the Commission, Member States, and the whole industry value chain. The new strategy for a better internet for kids (BIK+), adopted on 11 May 2022, will ensure that children are protected, respected, and empowered online in the new Digital Decade, in line with the European Digital Principles. A child-friendly version of the BIK+ strategy has also been produced. This new strategy builds on the first European Strategy for a Better Internet for Children (BIK). As much has changed technologically and in EU legislation since 2012, a compendium of relevant legislation is available. BIK+ is the digital arm of the comprehensive EU Strategy on the Rights of the Child from 2021. Find out more on the European Commission's website.

17 For more see: https://saferinternet.hu/oldalak/safer-internet-center (Accessed: 10 January 2024).

18 For more see: https://better-internet-for-kids.europa.eu/en/bik (Accessed: 10 January 2024).

In reaching this point, European Commission policy has evolved over the course of several years and via various programmes.

> 'To help track this process, we have developed a policy roadmap aiming to provide a chronological overview of the various relevant activity lines and stakeholders involved, including programme timelines, key outreach events and campaigns, and the role of industry, as well as the ongoing evaluation processes.'[19]

5.2. The Impact of the Pandemic on Child Online Protection

The pandemic situation has also prompted new measures in education and training across the European Union.[20] The European Commission has put forward a Digital Agenda for Education (2021-2027), outlining its vision for high-quality, inclusive, and accessible digital education in Europe. It calls for action for closer cooperation at the European level to build on the lessons learnt from the recent outbreak of the coronavirus, which has mobilised technology for education and training at an unprecedented level and prepared education and training systems for the digital age.

5.3. Digital Data Protection – The GDPR Story

The advent of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), commonly known as the GDPR, has given new energy to data protection. While most people used to take the rules on data processing lightly, the new and uniform provisions currently in force have prompted everyone to delve deeper into the subject. The existing rules have been replaced by new ones, and I see that people are starting to pay more attention to what data they give, to whom, and when. As in any other area of life, the rules on children have been given a separate chapter with the following provisions.

The GDPR provides an enhanced level of protection for children's personal data and places increased obligations on data controllers who process children's data during their activities.

> 'Children merit specific protection regarding their personal data, as they may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing of personal data.
>
> In particular, such specific protection should apply to the use of children's personal data for the purposes of marketing or creating personality or user

19 Ibid.
20 More details: European Commission, 2020.

> profiles and the collection of personal data regarding children when using services offered directly to a child.
>
> The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.'[21]

Taking the above legislative detail as a starting point, let us look at the specific provisions in the GDPR to protect children's data.

The controller must act with particular care and apply the balancing of interests test where it intends to rely on legitimate interests as the legal basis for its processing (Article 6(1)(f)) and the data subjects of the processing are or may be children.

The regulation contains specific rules on the conditions for the consent of a child to the use of information society services (Article 8). Accordingly, in the case of processing based on consent, the processing of personal data in relation to information society services offered directly to children is lawful when, as a rule, the child is at least 16 years old. In the case of children under the age of 16, the processing of personal data of children is lawful only if and to the extent that consent has been given or authorised by the person having parental authority over the child. However, Member States may set a lower age, but not lower than 13 years. The controller must make reasonable efforts to verify that the consent has been given or authorised by the holder of parental responsibility over the child. When providing information, controllers should endeavour to provide the information in a concise, transparent, intelligible, and easily accessible form, in clear and plain language, where the recipient of the information is a child.

The Central European countries presented set the following ages for the child's contribution: a) Czech Republic – age 13; b) Hungary – age 16; c) Poland – age 13; d) Slovak Republic – age 16.

5.4. European Union Priorities

Child sexual abuse is a real and growing threat. Abusers are increasingly using the Internet to communicate with each other, share material with others and contact children. Predators take photos and videos of their crimes and share them online. They use intimidation and blackmail to force children to commit sexual acts, which is impermissible and illegal. They use a variety of tools: webcams, mobile phones, social media, and other online platforms.

The European Commission proposes to adopt new EU legislation[22] to help EU countries: detect and report online child sexual abuse; report and detect, report and prevent online child sexual abuse; report, prevent, and stop child sexual abuse.

The proposed legislation will make it mandatory for service providers to report online child sexual abuse on their platforms and alert the authorities so that predators

21 European Parliament and the Council, 2016, Recital 38.
22 European Commission, 2022.

can be brought to justice. The proposal also requires service providers to report cases of child grooming – where sexual predators develop trusting and emotional relationships with children to manipulate, exploit, and abuse them.[23]

In addition to this pressing issue, the EU is also trying to respond to new technological innovation with uniform rules. A good example is the establishment of common ground rules on artificial intelligence.[24] Additionally, consider the recently passed Digital Services Act, which allows for greater online protection for children as consumers.[25]

6. Child Protection in Central Europe

The previous chapters have introduced the basic concepts and the current digital landscape. It is time to take a closer look at what child online protection looks like in practice in the Central European region.

6.1. Similarities in Child Online Protection in Central Europe

Through shared historical traditions, geographical proximity, economic, and other forms of cooperation, the four countries described above all share a common concern for the online protection of children and young people. All four countries are party to the oldest international convention protecting children, the UN Convention on the Rights of the Child.[26] In a short time after the simultaneous regime changes, they all incorporated the international instrument focusing on the protection of children into their own legal systems and developed institutional arrangements to put it into practice.

In response to a changing world, the Convention on the Rights of the Child has been updated over the years with new commentaries. In response to the changing digital world, General Comment No. 25 on children's rights in the digital environment[27] was published in 2021. With this, the UN formalised that children's rights also apply online. The transposition of the Commentaries into national law is no longer progressing with the same popularity and speed as the 1989 basic convention. None of the countries presented has transposed this new and, in my view, inescapable legal mandate for the 21st century into its everyday practice. It is, however, undeniable that the exercise of digital rights in everyday life is tacitly seen as a fundamental right in all four countries.

23 European Commission, 2024.
24 European Parliament, 2023.
25 Anonymus, n.d.
26 United Nations General Assembly (1989) Convention on the Rights of the Child, New York, 20 November [Online]. Available at: https://www.unicef.org/child-rights-convention/convention-text (Accessed: 10 January 2024).
27 See: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/053/43/PDF/G2105343.pdf?OpenElement (Accessed: 10 January 2025).

All four countries have a cybersecurity plan, legislation, and institutional framework in place. In these action plans, provisions for children are specifically mentioned. This means that all four countries are taking priority actions to keep children safe online and to strengthen the role of digital media literacy in education.

Having reviewed the similarities, it is time to look at some specific good examples and good practices in each country in child online protection.

6.2. Specific Success Stories

The other chapters of the book provide a detailed legal and institutional background of the countries of the Eastern European region, so I will just highlight a digital good practice example in this chapter.

6.2.1. Child Online Protection in Czech Republic

The Safer Internet Consortium of the Czech Republic has a strong influence on policy making. They are active players in the European circular flow and are also good advocates in their own countries. Their current priority for more effective public action is to push for action against online child sexual abuse.[28]

6.2.2. Child Online Protection in Hungary

The latest element of the Hungarian legislative and institutional system is the Digital Strategy for Child Protection. The institution responsible for the implementation of the strategy[29] and the professionals working within it state their credo as follows.

One of the most important issues in the digital transformation is how we can use the Internet, especially how young people can use the Internet safely, consciously and in a value-creating way.

To eliminate the risks to our children while using the Internet and to take advantage of the opportunities offered by the Internet, we place great emphasis on digital media literacy, meaning creating conditions for safe Internet use for children in a conscious and value-creating way.[30]

6.2.3. Child Online Protection in Poland

Of the four countries presented, Poland's specific child protection measures should be highlighted in the context of the children's ombudsman. It was established by the Law on the Ombudsman for Children passed on 6 January 2000, implementing article 72(4) of the Constitution of the Republic of Poland. In its day-to-day work, the Ombudsman for Children's Rights focuses on the following children's rights: the right to life and health care; the right to education within the family; the right to a decent standard of living; the right to education; the rights of children with disabilities; protection of

28 Safer Internet Center of the Czech Republic [Online]. Available at: https://www.bezpecnyinternet.cz/en/about-us/ (Accessed: 10 January 2024).
29 Details of the Strategy see: https://digitalisgyermekvedelem.hu/en/home/ (Accessed: 10 January 2024).
30 Ibid.

children against violence, cruelty, exploitation, moral decay, neglect, and other forms of abuse.[31]

6.2.4. Child Online Protection in the Slovak Republic

In the Slovak Republic, the Safer Internet Consortium is also a priority. Among their educational materials for preschoolers and schoolchildren, I would like to mention the short films with lambs, which are very popular all over Europe and are available free of charge in several European languages.[32] Using the characters of Slovak folktale heroes such as the shepherd, sheep, wolf, and hunter, they have created stories about everyday life in the digital world.

7. Summary, Looking to the Future

After reviewing the EU and national institutional and legal frameworks, it is time to take stock of whether these frameworks are providing maximum protection for children online. It is certainly positive that the child online protection is a high priority at both the European and national levels. There is a diverse, subject-specific legal environment and institutional framework at the disposal of each country to ensure the full development of child protection online. This sentence suggests that all is well. However, the situation is not so rosy. Existing legislation tries to fully meet the challenges of the online space, but does not always deliver the expected results, such as a reduction in the number of cases, deregulation, new legislation, or updating of existing legislation.

EU legislation is very slow, despite the drive for a single set of rules. By the time a regulation is adopted, technology is at least two or three steps ahead of it, and we have not even added the time taken for national implementations. It is like taking a sieve to water. However, there is a great need to establish a common regulatory framework for child online protection issues (see GDPR regulation), as the Internet does not recognise borders; therefore, in cross-border cases, common action is essential to provide assistance as quickly and efficiently as possible.

Child online protection issues are and have been a primary focus of civic sensitivity. They are the ones who see a situation at first hand. They react immediately to what is happening through campaigns and awareness-raising actions. Their free content makes them popular with a wide section of society. However, limited financial resources do not allow them to provide answers to all child online protection questions. Civil society initiatives need to be given greater visibility through close cooperation between public and corporate actors. Such joint cooperations can also be a catalyst for legal change while pooling knowledge and experience.

31 More details: https://brpd.gov.pl/kontakt/ (Accessed: 10 January 2024); https://brpd.gov.pl/o-rzeczniczce/ (Accessed: 10 January 2024).

32 See: http://sk.sheeplive.eu/en (Accessed: 10 January 2024).

The cause of child online protection is a never-ending mission for anyone who has ever been passionate about children. There are always new challenges ahead. With technology advancing at record speed, the law will always be lagging. The term "digital divide", as it is known in the online world, refers not only to the different levels of digital knowledge between generations but also to the imaginary boundary between the current regulatory environment and the Internet. The world of law alone will not give us complete digital security, but it will bring us one step closer. The last decade has seen an explosion of technological progress, and it is far from over. Creating a safe, positive, and valuable online experience is something we all share!

Bibliography

Anonymus (n.d.) 'Digital Service Act (DSA) – Updates, Compliance' [Online]. Available at: https://www.eu-digital-services-act.com/ (Accessed: 10 January 2024).

Council of Europe (2016) 'Digital Citizenship Education' [Online]. Available at: www.coe.int/en/web/digital-citizenship-education/home (Accessed: 10 January 2024).

European Commission (2020) 'Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Digital Education Action Plan 2021-2027 Resetting education and training for the digital age, 30 September 2020, COM (2020)624 final' [Online]. Available at: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_hu (Accessed: 10 January 2024).

European Commission (2022) 'Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse', 11 May 2022, COM (2022)209 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN (Accessed: 10 January 2024).

European Commission (2024) '#EUvsChildSexual Abuse - Campaign to prevent and combat child sexual abuse', *home.affaires.ec.europa.eu,* 20 February [Online]. Available at: https://home-affairs.ec.europa.eu/whats-new/communication-campaigns/euvschildsexual-abuse-campaign-prevent-and-combat-child-sexual-abuse_en (Accessed: 10 January 2024).

European Parliament and the Council (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' [Online]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (Accessed: 10 January 2024).

European Parliament (2023) 'Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI', *europarl.europa.eu*, 9 December [Online]. Available at: https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai (Accessed: 10 January 2024).

Farkas, B.P. (2016) 'Digitális intelligencia – Készségek a sikeres digitális élethez', *Tér/Idő,* 4 September [Online]. Available at: https://terido.wordpress.com/2016/09/04/digitalis-intelligencia-keszsegek-a-sikeres-digitalis-elethez/ (Accessed: 10 January 2024).

International Telecommunication Union (2019) 'Measuring digital development – Facts and figures 2019' [Online]. Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (Accessed: 10 January 2024).

International Telecommunication Union (2020a) *Guidelines for policy-makers on Child Online Protection*. Geneva: International Telecommunication Union [Online]. Available at: https://www.itu-cop-guidelines.com/policymakers (Accessed: 10 January 2024).

International Telecommunication Union (2020b) *Guidelines for Parents and Educators.* Geneva: International Telecommunication Union [Online]. Available at: https://www.itu-cop-guidelines.com/parentsandeducators (Accessed: 10 January 2024).

International Telecommunication Union (2020c) 'Global Cybersecurity Agenda (GCA)' [Online]. Available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (Accessed: 10 January 2024).

International Telecommunication Union (2020d) 'Measuring the Information Society Report – Executive Summary 2018' [Online]. Available at: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf (Accessed: 10 January 2024).

Livingstone, S., Carr, J., Byrne, J. (2015) 'One in three: The task for global internet governance in addressing children's rights' *Global Commission on Internet Governance: Paper Series,* 2015/22, pp. 1–32 [Online]. Available at: https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights (Accessed: 10 January 2024).

Sey, A., Hafkin, N. (eds.) (2019) *Taking stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership – Report of EQUALS Research Group, led by the United Nations University.* Macau: United Nations University Institute on Computing and Society/International Telecommunications Union [Online]. Available at: https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf (Accessed: 10 January 2024).

UNICEF (2017) *The State of the World's Children 2017: Children in a Digital World*. New York: UNICEF [Online]. Available at: https://www.unicef.org/uzbekistan/media/711/file/SOWC:%20Children%20in%20a%20Digital%20World.pdf (Accessed: 10 January 2024).

UNICEF (2019) *Growing up in a connected world*. Florence: UNICEF Office of Research – Innocenti [Online]. Available at: https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf (Accessed: 10 January 2024).

United Nations General Assembly (1989) Convention on the Rights of the Child, New York, 20 November [Online]. Available at: https://www.unicef.org/child-rights-convention/convention-text (Accessed: 10 January 2024).