

| CHILDREN IN DIGITAL AGE |

Human Rights – Children’s Rights VI

ISSN 3058-0161 (print)

ISSN 3094-371X (online)

International and Comparative Children’s Rights 6

ISSN 3058-0293 (print)

ISSN 3094-3728 (online)

CHILDREN IN DIGITAL AGE

Edited by
Csenge HALÁSZ



MISKOLC – BUDAPEST | 2025

Children in Digital Age

ISBN 978-615-7027-11-4 (printed version)

ISBN 978-615-7027-12-1 (pdf)

ISBN 978-615-7027-13-8 (epub)

<https://doi.org/10.71009/2025.csh.cida>



Published by

© **Central European Academic Publishing**

(Miskolc – Budapest, Hungary)

1122 Budapest, Városmajor St. 12 (Hungary)

All rights are reserved by the Central European Academic Publishing.

Design, layout

PÁTRIA PRINTING HOUSE CO.

Chief executive officer: Katalin Orgován

Printed and bound by

EDITOR-IN-CHIEF OF THE SERIES

János Ede SZILÁGYI – Strategy Director of the Central European Academy; Professor, University of Miskolc, Hungary

SERIES EDITORS

Marek ANDRZEJEWSKI – Professor, Institute of Legal Studies of the Polish Academy of Sciences; Head of the Family Law and Child Law Centre, Poland

Tímea BARZÓ – Director-General, Central European Academy; Professor, University of Miskolc, Hungary

Márta BENYUSZ – Head of the Institute for Children’s Rights and Family Law, Central European Academy; President, Association for Children’s Rights, Hungary

Tanja KARAKAMISHEVA-JOVANOVSKA – Professor, Ss. Cyril and Methodius University in Skopje, Republic of Macedonia

Enikő KRAJNYÁK – Head of the Institute for Human Rights and European Law, Central European Academy; Assistant Professor, University of Miskolc, Hungary

Aleksandra KORAĆ GRAOVAC – Professor, University of Zagreb, Croatia

Péter KOVÁCS – Professor, Pázmány Péter Catholic University, Hungary; Retired Judge, International Criminal Court, Netherlands

Mariusz MUSZYŃSKI – University Professor, Cardinal Stefan Wyszyński University in Warsaw; Retired Judge, Constitutional Tribunal of the Republic of Poland, Poland

Péter PACZOLAY – Professor Emeritus, University of Szeged, Hungary; Judge, European Court of Human Rights, France

Vladan PETROV – Professor, University of Belgrade, Serbia; Judge, Serbian Constitutional Court, Serbia; Member of the Venice Commission, Italy

Anikó RAISZ – Associate Professor, University of Miskolc, Hungary

Vasilka SANCIN – Professor, University of Ljubljana, Slovenia; Judge, European Court of Human Rights, France

Frane STANIČIĆ – Professor, University of Zagreb; President, Constitutional Court of the Republic of Croatia, Croatia

Katarzyna ZOMBORY – Director of Research, Central European Academy, Hungary

MEMBERS OF THE INTERNATIONAL ADVISORY BOARD

Petar BAČIĆ – Professor, University of Split, Croatia

Gyula BÁNDI – Professor Emeritus, Pázmány Péter Catholic University, till 2029 Deputy-Commissioner for Fundamental Rights, Ombudsman for Future Generations

Károly BENKE – First-assistant-magistrate of the Constitutional Court of Romania; Head of the Constitutional Law Department within the National Institute of Magistracy

Nóra BÉRES – Assistant Professor, University of Miskolc, Hungary

Sibilla BULETSA – Professor, Head of the Department of Civil Law and Civil Procedure, Uzhhorod National University, Ukraine

Doina CAZACU – Associate Professor, State University of Moldova, Moldova

Jakub CZEPEK – University Professor, Cardinal Stefan Wyszyński University in Warsaw; Member of the UN Subcommittee on Prevention of Torture, Poland

Sanja ĐAJIĆ – Professor, University of Novi Sad School of Law, Serbia

Olga DORUL – Associate Professor, Moldova State University, Moldova; Associate Professor, “Dunarea de Jos” University of Galati, Romania

Benjamin FLANDER – Associate Professor, University of Maribor, Slovenia

Kateřina FRUMAROVÁ – Associate Professor, Palacký University, Czech Republic

Lilla GARAYOVÁ – Vice-Dean, Associate Professor, Pan-European University; Associate Professor, Comenius University, Slovakia

Rebecca Lilla HASSANOVÁ – Assistant Professor, Pan-European University, Slovakia

Dubravka HRABAR – Professor, University of Zagreb, Faculty of Law, Croatia

Ivan JOKANIVIĆ – Senior Researcher, Central European Academy, Hungary

Gordana KOVAČEK STANIĆ – Retired Professor, University of Novi Sad, Serbia

Laura KOVÁCS-BERÉNYI – Assistant Professor, University of Miskolc, Hungary

Suzana KRALJIĆ – Professor, University of Maribor, Slovenia

Zdeňka KRÁLÍČKOVÁ – Professor, Masaryk University, Czech Republic

Alena KRUNKOVÁ – Vice-Dean, Associate Professor, Pavol Jozef Šafárik University, Slovakia

Bartosz LEWANDOWSKI – Senior Researcher, Central European Academy, Hungary

Roland LINDT – Assistant Professor, University of Miskolc, Hungary

Wojciech LIS – University Professor, The John Paul II Catholic University of Lublin, Poland

Bartosz MAJCHRZAK – University Professor, Cardinal Stefan Wyszyński University in Warsaw, Poland

György MARINKÁS – Associate Professor, University of Miskolc, Hungary

Jozef MIKLOŠKO – Commissioner for Children, Slovakia

Zsófia NAGY – Senior Researcher, Central European Academy, Hungary

Bartłomiej OREŻIAK – Assistant Professor, Cardinal Stefan Wyszyński University in Warsaw, Poland

Teodor PAPUC – Lecturer, State University of Moldova; Deputy Chief Secretary, Constitutional Court of the Republic of Moldova, Moldova

Natasa PLAUSIC – Judge, Constitutional Court of Serbia, Serbia

Peter POTÁŠCH – Professor, Pan-European University; Judge, Supreme Administrative Court of the Slovak Republic, Slovakia

Kata Zsófia PRÉM – PhD Student, University of Miskolc, Hungary

Marieta SAFTA – Professor, Titu Maiorescu University; Member of the Doctoral School, University of Economic Studies (ASE), Romania

Erzsébet SÁNDOR-SZALAY – Professor, University Babes-Bolyai, Romania; Professor, University of Pécs, Hungary; Ordinary member of the Advisory Committee of the FCNM (CoE)

David SEHNÁLEK – Vice-Dean, Associate Professor, Masaryk University, Czech Republic

Ivan ŠIMOVIĆ – Associate Professor, University of Zagreb, Croatia

Eka SIRADZE – Associate Professor, Jean Monnet Center of Excellence, Tbilisi State University, Georgia

Milan ŠKULIĆ – Professor, University of Belgrade; Judge, Constitutional Court of Serbia, Serbia
Katarína ŠMIGOVÁ – Dean, Associate Professor, Pan-European University, Slovakia
Paweł SOBCZYK – University Professor, University of Opole, Poland
Grega STRBAN – Professor, University of Ljubljana, Slovenia; Senior Research Associate, University of Johannesburg; Member of the European Committee of Social Rights, Council of Europe
Aleksandra SYRYT – University Professor, Cardinal Stefan Wyszyński University in Warsaw, Poland
Krzysztof SZCZUCKI – University Professor, University of Warsaw, Poland
Szilárd SZTRANYICZKI – Vice-Rector, Associate Professor, Sapientia Hungarian University of Transylvania, Romania
Tudorel TOADER – Professor, Alexandru Ioan Cuza University, Retired Judge of the Constitutional Court of Romania, Romania
Juraj VAČOK – Professor, Comenius University in Bratislava, Judge, the Supreme Administrative Court of the Slovak Republic, Slovakia
Magdolna VALLASEK – Associate Professor, Sapientia Hungarian University of Transylvania, Romania
Mario VINKOVIĆ – Professor, University of Osijek, Croatia; Member of the European Committee of Social Rights; Head of the Institute for Labour and Social Legislation, Social Work and Foreign Languages
Agnieszka WEDEŁ-DOMARADZKA – University Professor, Kazimierz Wielki University, Poland
Marcin WIELEC – University Professor, Vice Dean, Cardinal Stefan Wyszyński University in Warsaw, Poland

BOOK SERIES MANAGERS

Kata Zsófia PRÉM – University of Miskolc, Hungary
Laura KOVÁCS-BERÉNYI – University of Miskolc, Hungary

DESCRIPTION

CEA Publishing's 'Human Rights – Children's Rights' book series is inspired by the idea that the universality and indivisibility of human rights can still accommodate a regional perspective on human rights protection. Different collective identities, sensitivities, and historical backgrounds may lead to different emphases on certain human rights issues, reflecting the cultural and legal heritage of Central and Eastern Europe.

Although the series is primarily law-focused, it also embraces an interdisciplinary approach and therefore includes contributions from other academic fields.

The main areas of law covered in the series are human rights, children's rights, and the rule of law, as well as other areas of law that help ensure their effective implementation. A prominent feature of the series is its examination of the legal systems and jurisprudence of Central and Eastern European countries, though not exclusively so. As the series aims to provide useful legal knowledge to non-lawyers, it also offers general legal background necessary to understand the subject matter.

The series is divided into two distinct sub-series, each numbered separately. One sub-series is entitled 'Human Rights and Rule of Law' (HRRL) and the other 'International and Comparative Children's Rights' (ICCR). Regarding their relationship, HRRL is considered the more general sub-series, while ICCR focuses on more specific themes.

Other titles in the book series
Human Rights – Children's Rights

2024

Márta Benyusz – Anikó Raisz (eds.):
International Children's Rights

Anikó Raisz (ed.):
Children's Rights in Regional Human Rights Systems

2025

Bernadett Raposa – Balázs Péter Hámornik (eds.):
Social and Personality Development in Childhood

Katarzyna Zombory – Márta Benyusz (eds.):
Religion and Children's Rights

Nóra Jakab – Márta Benyusz (eds.):
Child-Protection Systems

| CONTENTS |

13		CHAPTER 1 – Children in Digital Age – Introduction (<i>Csenge HALÁSZ</i>)
25		CHAPTER 2 – The Impact of Individual Online Platforms on Children’s Psychological Development (<i>Dominik GOŁUCH</i>)
49		CHAPTER 3 – Children in Digital Age – International Regulations (<i>Sanja SAVČIĆ</i>)
67		CHAPTER 4 – European Law (<i>András KOLTAY</i>)
87		CHAPTER 5 – Children in Digital Age – European Union and Central European Best Practices and Challenges (<i>Katalin BARACSI</i>)
105		CHAPTER 6 – Children in Digital Age – Croatian Perspective (<i>Hrvoje LISIČAR</i>)
129		CHAPTER 7 – Children in Digital Age – Czech Perspective (<i>Lenka WESTPHALOVÁ</i>)
153		CHAPTER 8 – Children in Digital Age – Hungarian Perspective (<i>Csenge HALÁSZ</i>)
171		CHAPTER 9 – Children in Digital Age – Polish Perspective (<i>Agnieszka GRYSZCZYŃSKA</i>)
199		CHAPTER 10 – Children in Digital Age – Romanian Perspective (<i>Zsolt KOKOLY</i>)
223		CHAPTER 11 – Children in Digital Age – Serbian Perspective (<i>Sanja SAVČIĆ</i>)
245		CHAPTER 12 – Children in Digital Age – Slovakian Perspective (<i>Péter KOROMHÁZ</i>)
265		CHAPTER 13 – Children in Digital Age – Slovenian Perspective (<i>Benjamin LESJAK</i>)
291		CHAPTER 14 – Children in Digital Age – Summary (<i>Csenge HALÁSZ</i>)
309		COLLECTION OF TERMS

| EDITOR |

Csenge HALÁSZ

Assistant Professor, University of Miskolc, Hungary

| AUTHORS |

Katalin BARACSI

Lawyer, Social Media Trainer, Hungary

Dominik GOŁUCH

Assistant Professor, Vice Dean for Student Affairs and Education, Cardinal Stefan Wyszyński University in Warsaw, Poland

Agnieszka GRYSZCZYŃSKA

Professor, Cardinal Stefan Wyszyński University in Warsaw, Poland

Csenge HALÁSZ

Assistant Professor, University of Miskolc, Hungary

Zsolt KOKOLY

Assistant Professor, Sapientia Hungarian University of Transylvania, Romania

András KOLTAY

Research Professor, University of Public Service; Professor, Pázmány Péter Catholic University, Hungary

Péter KOROMHÁZ

Assistant Professor, Pavol Jozef Šafárik University, Slovakia

Benjamin LESJAK

Associate Professor, University of Primorska, Slovenia

Hrvoje LISIČAR

Professor, University of Zagreb, Croatia

Sanja SAVČIĆ

Professor, University of Novi Sad, Serbia

Lenka WESTPHALOVÁ
Assistant Professor, Palacký University Olomouc, Czech Republic

| REVIEWERS |

Attila DUDÁS
Professor, University of Novi Sad, Serbia

Melinda HAL
Clinical Psychologist; Research Director, Learning Institute,
Mathias Corvinus Collegium, Hungary

Suzana KRALJIĆ
Professor, University of Maribor, Slovenia

Réka LACZKÓ
Associate Professor, Babeş-Bolyai University, Romania

Alexandra LÖWY
Associate Professor, Comenius University, Slovakia

Dušan POPOVIĆ
Professor, University of Belgrade, Serbia

Ana RADINA
Assistant Professor, University of Split, Croatia

David SEHNÁLEK
Vice-Dean, Associate Professor, Masaryk University, Czech Republic

Julianna Sára TRASER
Head of Department, Ferenc Mádl Institute of Comparative Law, Hungary

Marzena TOUMI
Professor, War Studies University in Warsaw, Poland

Nelli Edina VARGA
Assistant Professor, University of Debrecen, Hungary

| TECHNICAL EDITOR |

Petra FRÁTER-BIHARI

PhD Student, Deák Ferenc Doctoral School of Law, University of Miskolc, Hungary

Children in Digital Age

Introduction

Csenge HALÁSZ

“Instead of the unlimited freedom promised by the internet, are our children (...) really threatened with total control at the price of virtual presence and a fully digital world? Are they the victims of a huge, greedy marketing machine that is invading the world from all directions? They are only in danger if they do not understand this brave new media world. That is why we must explain it to them so that they can see it clearly. Every single time.”

/Melissa Müller/

1. Children Online – Statistics and Recommendations

The use of various digital tools, which can be seen as *the “key”* to accessing certain online platforms, is nowadays a clear feature of people’s lives. The various “*smart devices*” are practically integrated into everyday, routine activities. This term refers to various devices and appliances that have an IP address and are able to send and receive data over the Internet network. To give just a few examples, a smart device could be a mobile phone or a computer, but also a television or a clock, or even a dishwasher, if they are uniquely identifiable and capable of transmitting data over the Internet.¹

Obviously, the various smartphones and PCs play a prominent role in accessing certain Internet interfaces. Thanks to their small size and their extremely fast data

1 Online Encyclopedia of Public Services, n.d.

Csenge Halász (2025) ‘Children in Digital Age – Introduction’ in Halász, Cs. (ed.) (2025) *Children in Digital Age*. Miskolc–Budapest: Central European Academic Publishing, pp. 13–23. https://doi.org/10.71009/2025.csh.cida_1.

reception and transmission capabilities, smartphones have become practically an almost obligatory “accessory” for individuals. The primary function of these devices is beginning to lose its importance, given that they are used primarily to connect to the World Wide Web. According to statistics, in 2014, around 1 billion people globally used smartphones, by 2024 this will exceed 5 billion and by 2027 it could reach 6 billion.²

According to research also published in 2024, more than 90% of children use some kind of smart device, and nine out of ten children under the age of eleven regularly use internet-connected devices.³ Similarly instructive data was published in late 2023, based on a sample of ninety children.⁴ One of the key findings of the research is that the number of children using smart devices increases steadily with age. Another significant finding is that by the time children reach the age of eighteen months, the majority of them have already been exposed to screen-based media, which in most cases means using mobile phones rather than television.

Also worth mentioning is a study from 2022, which includes age-specific findings on children’s screen time, with children under two spending an average of forty-nine minutes a day in front of a screen, and children aged between five and eight spending more than three hours. Children aged between eight and twelve spend an average of five hours a day using smart devices, while for teenagers the figure is close to eight hours a day.⁵

These statistics show that the time spent in front of a screen by people under the age of eighteen has increased dramatically over the past few years, due to a number of social phenomena. One of these is the COVID-19 epidemic, during which smart devices have become the main means of entertainment and communication. In response to this phenomenon, the World Health Organisation (WHO) has issued a recommendation specifically targeting children’s screen time. According to this recommendation, excessive screen time can clearly have negative health effects, and banning children from using smart devices is not a fully adequate solution, given that an important part of their development involves learning to use different digital devices.⁶ It is recommended that it is crucial that children learn at an early age to strike a healthy balance between the use of digital devices, adequate physical activity and quality sleep. Parents of children naturally have a key role to play in ensuring this and in establishing regularity. In terms of screen time, the WHO’s principles suggest that no minimum level of smart device use is recommended for children under two years of age, and that children between two and five years of age should be allowed a minimum level of one hour per day.⁷ For children over the age of six, the maximum amount of screen time should be set on an individual basis, in order to allow the

² Backlinko, 2024.

³ Woodhouse and Lalic, 2024.

⁴ Shah and Phadke, 2023.

⁵ Johnson, 2023.

⁶ WHO, 2019.

⁷ Ibid.

child time for adequate physical activity and to ensure that he or she has a quiet and adequate period of rest, which is essential for healthy development.

In our view, the recommendations made by the WHO are certainly necessary and adequately reflect the excessive screen use by children, as highlighted by the various statistics outlined above. From the data we have analysed, it can be concluded that children spend several times the daily screen time recommended by the World Health Organisation using various digital devices.

Another important question is what children use the various Internet access devices for. Younger children typically use their smartphones to play games, watch cartoons or other online programmes. As they grow older, this is replaced by social media use, as shown by the fact that, according to statistics published by the European Union in 2023, 84% of young people will use a social media platform, and 16 year olds will typically have a profile on at least three social media platforms.⁸

2. Specific Phenomena in the World of Social Media

*A public space of ideas, a “brave new world”, a global network, a digital agora.*⁹ These are just a few of the terms used to describe some of the global internet platforms that currently have more than 5.4 billion users worldwide.¹⁰ As part of the global social experience, users of a given portal can access information, share text and audiovisual content and interact with each other, spending several hours a day on each online platform, given that they are considered to be highly addictive platforms. However, social media sites cannot be grouped under a single umbrella, and there are several sub-types of social media sites. At global level, the Facebook platform¹¹, operated by Meta, is the market leader, but the most popular platforms for users under 18 are TikTok, Instagram and YouTube.¹²

Global online platforms typically link registration to the age of thirteen¹³, but it is common for children much younger to have a profile on a social networking site. Efforts are being made by social networking site operators to filter this out, for example Facebook has created a form that allows any user to report a profile that they suspect is used by a child under the age of thirteen, but the effectiveness of these methods is questionable as children can re-register on social networking sites by providing false information.¹⁴

8 Eurostat, n.d.

9 See also: Barzó, Csák and Czékmann (eds.), 2021.

10 Petrosyan, 2025.

11 Buffer, 2025.

12 Anderson, Faverio and Gottfried, 2023.

13 See for example the terms of use of Facebook and YouTube.

14 See: How can I report a child under 13 on Facebook? [Online]. Available at: <https://www.facebook.com/help/157793540954833> (Accessed: 3 August 2024).

The moment a person, even a child, registers on a social networking platform, a contractual relationship is established between him/her and the operator of the social networking site, which can be classified as a contract between a consumer and a third party, concluded between the parties at a distance, under general contractual conditions, for the provision of an electronic service. The transaction therefore involves the immanent contractual conditions and the various rules and regulations set by the service provider, which are known to a very small number of users. The children and young people who register on social networking sites are therefore part of an online community space that is unilaterally shaped by a set of rules, and are therefore vulnerable to certain specific phenomena that are typical of the online space.

The first of these is *cyberbullying*¹⁵, the phenomenon of cyberbullying, which typically affects teenagers. According to a UNICEF survey, one in three teenagers has been bullied on a social media platform.¹⁶ According to research conducted by the Pew Research Center, 46% of teenagers regularly experience some form of harassment online, mostly in the form of abusive language, unsolicited messages and untruthful rumours.¹⁷

In response to this phenomenon, the European Union has published a series of information materials and draft regulations¹⁸, and UNICEF launched a campaign on TikTok 2021 to raise awareness of the dangers of this phenomenon with the help of young opinion leaders.¹⁹

Another *issue* worth highlighting in relation to social platforms, including children, is the *zero-price business model*, which is essentially the idea that social networking sites display targeted ads in the news feed of individual users, thereby increasing the revenue of the companies that post the ads.²⁰ The algorithms used by the various social media sites display content to individual users that is likely to trigger some kind of interaction from each user, such as liking, sharing or commenting on the content. As a consequence, underage users are highly exposed to different types of advertising, which may not even be appropriate to their age and maturity level, but also to the proliferation of different *trends* and *challenges* on the Internet.

In recent years, a number of viral online “*challenges*” have begun to spread, which have also been associated with a number of health risks. One example, to name but a few, was the Cinnamon Challenge, which involved participants trying to swallow a teaspoonful of cinnamon on camera, which was extremely irritating to the mucous membranes, leading to severe sneezing, coughing and choking.²¹ A similar principle

15 It is worth highlighting here that there is a very broad literature on the phenomenon of cyberbullying, mainly from the perspective of criminal law. UNICEF, n.d.a.; Pongó, 2021; Marinkás, 2023.

16 UNICEF, n.d.a.

17 Strandell, 2024.

18 See for example: Murphy, 2024.

19 UNICEF, n.d.b.

20 GVH, 2020.

21 Cronan, 2013.

was followed in the so-called washing-up capsule challenge, which involved swallowing washing-up capsules, resulting in poisoning symptoms in many young people.²² More recently, a number of media outlets have covered the so-called blackout challenge, which involved the video maker holding his breath for so long that he eventually passed out. The challenge has sadly caused seven deaths worldwide.²³ There are several *differential characteristics* of these social media ‘trends’.

On the one hand, our reach is clearly linked to the TikTok platform, so we are clearly targeting a young age group, and the participants in the challenges were almost entirely young people aged between twelve and twenty-one. On the other hand, one explanation for the global spread of these fashionable and highly dangerous tasks is the FOMO “*fear of missing out*”, which is a manifestation of young people’s aspiration to be part of the community, which includes them.²⁴

Children who use social media are also very strongly affected by the problem of *fake news*, which is very similar to the challenges just mentioned in terms of spreading, and the formation of *opinion bubbles*. These two phenomena have a strong impact on children’s right to freedom of expression. The opinion bubble essentially means that a platform’s algorithms, after monitoring the user’s activity (e.g. the number of likes, comments, the number of pages visited), produce the content presented to it, creating a ‘*personalised public sphere*’ that can strongly shape the person’s opinion and influence his or her worldview. On the one hand, this is extremely convenient, as a child using social media is almost only exposed to content that is of interest to him or her, and on the other hand, much important news is not even delivered to him or her if the algorithms do not expect it to trigger the right amount of interaction.

The spread of fake news²⁵ is also being vigorously self-regulated by the various platforms, but from time to time, untrue information is being spread with incredible speed and reaches many children through social networking sites. In many cases, some of this untruthful information can cause distress to younger users whose intellectual development is not yet able to filter out information that is not true.

Another noteworthy problem is the phenomenon of *sharenting*, which has a very strong impact on children’s privacy rights. The term ‘*over-sharing*’ was first used in 2012 to refer to the excessive sharing of photographs and personal data of children,

22 Beyer, 2018.

23 Clark, 2022.

24 According to Lexiq: „FOMO is short for fear of missing out, which literally translates as fear of missing out. FOMO refers to the phenomenon of wanting to keep track of events and opportunities so as not to miss out on an entertainment, investment or other opportunity because you didn’t know about it in time or didn’t go when you had the chance.” [Online] Available at: <https://lexiq.hu/fomo> (Accessed: 23 June 2024). There is a very extensive literature on this phenomenon, see for example: Alutaybi et al., 2020; Tanhan, Özök and Tayiz, 2022.

25 A hoax is a piece of created information that is based on deliberate deception, disinformation or a hoax. Fake news producers consciously rely on people’s gullibility, naivety, digital illiteracy and those who face serious challenges in basic literacy. For an example of how fake news can be legally relevant, see: Funke and Flamini, n.d.

by combining the words ‘over-sharing’ and ‘parenting’.²⁶ The term, in a general sense, refers to behaviour where a parent posts large amounts of content about their child on social media. *Maja Sonne Damkjaer*, in a relevant study, identifies sharenting as a popular practice whereby parents share photos and news about their children.²⁷ *Stacey Steinberg*, a prominent expert on the topic,²⁸ identifies sharenting as an activity whereby parents post information about their children outside the so-called “family circle”. This could be a blog post on social media, or posting photos, videos or forwarding them via a messaging app.²⁹ In a study published in 2017 by the authors *Alicia Blum-Ross and Sonia Livingstone*, they identified sharenting as a form of self-representation by parents, which aims to share information about their children on social media.³⁰ According to *Charlotte Kay*, sharenting is when a parent or other relative of a child shares news, pictures or videos or other potentially sensitive information about their child on a social platform, typically Facebook or Instagram.³¹

For our part, we see sharenting as a phenomenon whereby parents or relatives post large amounts of detailed information about the child concerned in the form of photos, videos or text posts on social media, in violation of the child’s right to privacy.

The sharing of large amounts of detailed information is an essential element of the sharenting phenomenon, as illustrated by the fact that the term was originally coined to refer to over-posting by parents. In our view, sharenting can be achieved through the public sharing of both textual posts and photo and video recordings on social media platforms, which allow the child concerned to be identified. This problem, which is considered to be very common, requires a complex legal interpretation, which we will attempt to provide in this volume.

3. Aim of the Research and Structure of the Volume

Above, we have provided a thought-provoking overview of the statistics and emerging challenges that have a very strong impact on the rights of children who use the internet. The impact of the proliferation of global internet platforms as a social phenomenon, and the many positive and negative influencing factors that go hand in hand with it, are therefore a given, and the most important question is what legal instruments can be used to ensure that the rights of children who use the internet are protected.

26 The phrase was first used by Wall Street Journal journalist Steven Leckart in his op-ed „The Facebook-Free Baby” [Online]. Available at: <https://www.wsj.com/articles/SB10001424052702304451104577392041180138910> (Accessed: 22 July 2024).

27 Damkjaer, 2018, pp. 209–2018.

28 See also: Steinberg, 2017; Steinberg, 2024, pp. 148–190.

29 UNICEF, n.d.c.

30 Blum-Ross and Livingstone, 2017, pp. 110–125.

31 Kay, 2024.

In this volume, therefore, we aim to examine how the rights of children, a group that is highly vulnerable in terms of social media use and enforcement, are protected on different internet platforms, in relation to the ICCR LL.M. *“Children in digital age”*. *The research was interdisciplinary and comparative, examining the legal systems of Central and Eastern European countries.*

In order to establish the basis for the research, first the international legal background of the field will be explored, followed by a detailed analysis of the relevant European Union legislation. It is worth noting at the outset that a number of laudable initiatives have been taken recently at supranational level, both from a regulatory and a practical point of view, to ensure effective protection of the rights of children using the Internet. To take just one example, the European Union’s BIK+ (Better Internet for Kids) initiative³² celebrated its second birthday in May 2024. The initiative has also produced a number of easy-to-understand information materials, which have raised awareness of the dangers of the above-mentioned phenomena in a very graphic way.³³ But also worth highlighting are the publications for parents and teachers, which can help to promote good behaviour among those concerned.³⁴

After the presentation of supranational regulatory models, the country reports will be presented, including the relevant legislation and jurisprudence of Hungary, Romania, Serbia, Croatia, Poland, Czech Republic, Slovenia, Slovakia.

The chapters on each country are structured in a very similar way, in order to present each regulatory model in a logical and comparable way. The chapters begin with a discussion of the statistical data and legal definitions relevant to the country concerned. The rights of children that are typically and most frequently violated on the Internet are then discussed. These include the right to privacy and the right to be forgotten, the right to access information and education, the right to protection from abuse and the right to freedom of expression. The examination of these rights is not limited to a general description of the legal framework in a given country, but each chapter will focus on the typical Internet-specific rules affecting children as individuals. Following the discussion of the different rights, each chapter includes a discussion of cases that have arisen in connection with the exercise of children’s rights on the Internet. While not all the countries examined have relevant case law, valuable

32 European Commission, 2022.

33 E.g. European Commission, 2022; #SaferInternet4EU campaign [Online]. Available at: <https://www.betterinternetforkids.eu/saferinternet4eu> (Accessed: 23 June 2024), BIK #DigitalSun-Screen summer campaign: 10 tips to protect your family online during summer travels [Online]. Available at: <https://www.betterinternetforkids.eu/practice/awareness/article?id=7294297> (Accessed: 23 June 2024); Together for a better internet. [Online]. Available at: <https://www.saferinternetday.org/> (Accessed: 23 June 2024); Positive Online Content Awareness Month. [Online] Available at: <https://www.positiveonlinecontentforkids.eu/> (Accessed: 23 June 2024).

34 See: Creating a safer connected world: parents and carers [Online]. Available at: <https://www.betterinternetforkids.eu/hu/discover/parents-and-carers> (Accessed: 2 August 2024); Creating a safer connected world: teachers, educators and professionals [Online]. Available at: <https://www.betterinternetforkids.eu/hu/discover/teachers-and-educators> (Accessed: 2 August 2024).

lessons can be drawn from the case law presented in the volume. An intrinsic part of each country report is the presentation of the relevant state institutional system, i.e. whether a specific institution exists in a given state to ensure children's rights in the online world, and whether individual state institutions have adopted action plans or guidelines on this issue. Finally, each chapter contains a summary and conclusion on the legal system in the country concerned.

In view of the multidisciplinary nature of the subject "*Children in digital age*", this textbook includes a chapter on psychology, which uses the results of recent research to present in great detail the psychological effects of different internet platforms on children, with a special focus on social media sites. The author of the chapter distinguishes between positive and negative effects on children, highlighting the complexity of the field.

The volume concludes with a summary chapter and a glossary of terms, in order to provide a synthesis of the research results.

It is hoped that this volume, as well as helping to meet the requirements of the Children in digital age subject, will serve as a book of complex research for the law-seeking public. The subject is extremely topical and wide-ranging, and its importance is also for the protection of future generations, given that the broad rights of children on the Internet should not be eroded, and the protection of children who are also exposed to harmful influences is a very important task of the state, as well as of society and the family environment, defined as the smallest unit of society. The present volume reflects on this problem from a Central European perspective, for which special thanks are due to the authors András Koltay, Katalin Baracsi, Sanja Savčić, Zsolt Kokoly, Lenka Westphalová, Agnieszka Gryszczyńska, Dominik Gołuch, Hrvoje Lisičar, Benjamin Lesjak, Peter Koromhász.

Bibliography

- Alutaybi, A., et al. (2020) 'Combating Fear of Missing Out (FoMO) on Social Media: The FoMO-R Method', *International Journal of Environmental Research and Public Health*, 17(17), 6128; <https://doi.org/10.3390/ijerph17176128>.
- Anderson, M., Faverio, M., Gottfried, J. (2023) 'Teens, Social Media and Technology 2023', *Pew Research*, 11 December [Online]. Available at: <https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/> (Accessed: 3 August 2024).
- Backlinko (2024) 'Smartphone Usage Statistics'. Last updated March 13 2024. [Online]. Available at: <https://backlinko.com/smartphone-usage-statistics> (Accessed: 22 June 2024).
- Barzó, T., Csák, Cs., Czékmann, Zs. (eds.) (2021) „Gondolatok köztere”: A közösségi média személyiségvédelemmel összefüggő kihívásai és szabályozása az egyes államokban. Miskolc: University Press.
- Beyer, L. (2018) 'What is the Tide pod challenge and how did it start?', *Seattle Times*, 13 January [Online]. Available at: <https://www.seattletimes.com/nation-world/what-is-the-tide-pod-challenge-and-how-did-it-start/> (Accessed: 20 June 2024).
- Blum-Ross, A., Livingstone, S. (2017) 'Sharenting: parent blogging and the boundaries of the digital self', *Popular Communication*, 15(2), pp. 110–125; <https://doi.org/10.1080/15405702.2016.1223300>.
- Buffer (2025) '23 Top Social Media Sites to Consider for Your Brand in 2024', *buffer.com*, 21 May [Online]. Available at: <https://buffer.com/library/social-media-sites/> (Accessed: 4 July 2024).
- Clark, M. (2022) 'The TikTok, blackout challenge' has now allegedly killed seven kids', *The Verge*, 8 July [Online]. Available at: <https://www.theverge.com/2022/7/7/23199058/tiktok-lawsuits-blackout-challenge-children-death> (Accessed: 23 June 2024).
- Cronan, K.M. (2013) 'Is the „Cinnamon Challenge” Dangerous?', *Children's Minnesota* [Online]. Available at: <https://www.childrensmn.org/educationmaterials/parents/article/14035/is-the-cinnamon-challenge-dangerous/> (Accessed: 22 June 2024).
- Damkjaer, M.S. (2018) 'Sharenting = Good Parenting? Four Parental Approaches to Sharenting on Facebook' in Mascheroni, G., Ponte, C., Jorge, A. (eds.) *Digital Parenting. The Challenges for Families in the Digital Age*. Göteborg: Nordicom, pp. 209–218 [Online]. Available at: <https://www.diva-portal.org/smash/get/diva2:1535913/FULLTEXT01.pdf> (Accessed: 1 July 2024).
- European Commission (2022) 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Decade For Children And Youth: The New European Strategy For A Better Internet For Kids (BIK+) COM(2022)212 final' [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0212> (Accessed: 2 August 2024).

- Eurostat (n.d.) '96% of young people in the EU use the internet daily', *ec.europa.eu*, 14 July [Online]. Available at: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230714-1> (Accessed: 3 July 2024).
- Funke, D., Flamini, D. (n.d.) 'Most „Fake News” Legislation Risks Doing More Harm Than Good Amid a Record Number of Elections in 2024 – A guide to anti-misinformation actions around the world', *Poynter* [Online]. Available at: <https://www.poynter.org/ifcn/anti-misinformation-actions/> (Accessed: 2 July 2024).
- GVH (2020) 'A Gazdasági Versenyhivatal Facebook határozata – az ingyenesség ára' [Online]. Available at: <https://itki.uni-nke.hu/hirek/2020/01/13/a-gazdasagi-versenyhivatal-facebook-hatarozata-az-ingyenesseg-ara> (Accessed: 22 June 2024).
- Johnson, A. (2022) 'Screen time recommendations by age, *All About Vision*, 9 March [Online]. Available at: <https://www.allaboutvision.com/conditions/refractive-errors/screen-time-by-age/> (Accessed: 22 July 2024).
- Kay, C. (2024) 'Sharenting – should you post pictures of your children on social media?', *Weightmans.com*, 14 March [Online]. Available at: <https://www.weightmans.com/insights/sharenting-should-you-post-pictures-of-your-children-on-social-media/> (Accessed: 25 June 2024).
- Marinkás, Gy. (2023) 'Cyberbullying – EU-s háttér' in Nagy, Z. (ed.) *Az összehasonlító jog eszközével a gyűlölet ellen. Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Jogösszehasonlító Intézet, pp. 99–108; https://doi.org/10.47079/2023.nz.gyuloletbeszed.10_5.
- Murphy, C. (2024) 'Cyberbullying among young people: laws and policies in selected Member States' [Online]. Available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2024\)762331](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762331) (Accessed: 22 June 2024).
- Online Encyclopedia of Public Services (n.d.) 'Smart Tool' [Online] Available at: <https://lexikon.uni-nke.hu/szocikk/okos-eszkoz/> (Accessed: 22 June 2024).
- Petrosyan, A. (2025) 'Number of internet and social media users worldwide as of April 2024', *Statista*, 1 April [Online]. Available at: <https://www.statista.com/statistics/617136/digital-population-worldwide/> (Accessed: 5 July 2024).
- Pongó, T. (2021) *A cyberbullying és a diákok véleménynyilvánítási szabadsága, különös tekintettel az USA jogrendszerére*. Szeged: Iurisperitus [Online]. Available at: <https://publicatio.bibl.u-szeged.hu/25719/1/Pongo-04-20.pdf> (Accessed: 3 August 2024).
- Shah, S.A., Phadke, V.D. (2023) 'Mobile phone use by young children and parent's views on children's mobile phone usage', *Journal of Family Medicine and Primary Care*, 12(2), pp. 3351–3355 [Online]. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10866234/> (Accessed: 23 July 2024).
- Steinberg, S. (2017) 'Sharenting: Children's Privacy in the Age of Social Media', *Emory Law Journal*, 66(839) [Online]. Available at: <https://scholarship.law.ufl.edu/facultypub/779/> (Accessed: 2 July 2024).
- Steinberg, S. (2024) 'Children Seen but Not Heard', *Arizona Law Review*, 66(1), pp. 148–190 [Online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4445565 (Accessed: 12 July 2024).

- Strandell, J. (2024) 'What Is Cyberbullying and How Can It Be Stopped?', *Besedo*, 30 January [Online]. Available at: <https://besedo.com/blog/cyberbullying/> (Accessed: 21 June 2024).
- Tanhan, F., Özok, H.I., Tayiz, V. (2022) 'Fear of Missing Out (FoMO): A Current Review', *Psikiyatride Güncel Yaklaşımlar-Current Approaches in Psychiatry*, 14(1), pp. 74–85; <https://doi.org/10.18863/pgy.942431>.
- UNICEF (n.d.a.) 'Cyberbullying: What it is and how to stop it – What teens want to know about cyberbullying', *unicef.org* [Online]. Available at: <https://www.unicef.org/end-violence/how-to-stop-cyberbullying> (Accessed: 4 August 2024).
- UNICEF (n.d.b.) 'Együtt a sértő hangok ellen' [Online]. Available at: <https://unicef.hu/egyutt-a-serto-hangok-ellen> (Accessed: 22 June 2024).
- UNICEF (n.d.c.) 'What you need to know about „sharenting” Expert tips on protecting your child's privacy in the digital age', *unicef.org* [Online]. Available at: <https://www.unicef.org/parenting/child-care/sharenting> (Accessed: 25 June 2024).
- Woodhouse, J., Lalic, M. (2024) 'Social media and smartphone use by children', *House of Common Library*, February [Online]. Available at: <https://commonslibrary.parliament.uk/research-briefings/cdp-2024-0103/> (Accessed: 1 July 2024).
- WHO (2019) 'To grow up healthy, children need to sit less and play more', *who.int*, 24 April [Online]. Available at: <https://www.who.int/news/item/24-04-2019-to-grow-up-healthy-children-need-to-sit-less-and-play-more> (Accessed: 1 July 2024).

The Impact of Individual Online Platforms on Children's Psychological Development

Dominik GOŁUCH

ABSTRACT

In the era of digitalisation, online platforms have become an integral part of the lives of children and young people, playing a key role in their educational, social, and emotional development. This study aims to describe the potential impact of online platforms on the development of young users while showing the benefits and potential risks associated with their use. On the positive side, access to a wide range of educational resources and opportunities for social interaction via the Internet can support learning and the development of communication skills. Simultaneously, attention has been drawn to challenges, such as the risk of addiction, cyberbullying, and sleep disorders, which may result from the excessive and uncontrolled use of digital technologies. This study also highlights the importance of the role of adults – parents, teachers, and legislators – in creating a safe digital environment that promotes healthy online habits. Digital education, establishing rules for using the Internet, promoting off-screen physical activities and hobbies, and developing critical thinking about Internet content are recommended. It is important that adults are aware of the potential risks and actively support young people in safely using the Internet while building trust and openness to dialogue about their online experiences. Although online platforms offer young users numerous development opportunities, a conscious and balanced approach to using them is required. By promoting healthy digital habits and actively engaging adults in the digital education process, we can ensure that the Internet becomes a safe and valuable tool that supports the comprehensive development of children and youth.

KEYWORDS

development of children and youth, online security, digital education, excessive use of the Internet, online platforms, healthy digital habits

1. Introduction

In the face of dynamic technological progress, modern children are growing up in a world where the boundaries between reality and the virtual environment are increasingly blurred. Online platforms such as social media, educational portals, gaming applications, and video services have become an integral part of their lives, playing

Dominik GOŁUCH (2025) 'The Impact of Individual Online Platforms on Children's Psychological Development' in Halász, Cs. (ed.) (2025) *Children in Digital Age*. Miskolc–Budapest: Central European Academic Publishing, pp. 25–48. https://doi.org/10.71009/2025.csh.cida_2.



a key role not only in learning and acquiring knowledge but also in building social relationships and forming identity. Young users, who use a wide range of available digital tools, have incomparably greater opportunities to explore the world, express themselves, and establish contacts with peers from different corners of the world.

However, along with the undoubted benefits of using online platforms, there are also risks and challenges that can have far-reaching effects on a child's developing mind. Problems such as excessive internet use, the risk of exposure to inappropriate content, cyberbullying, and the impact of social media on self-esteem and mental well-being are just some of the issues that raise concerns among parents, teachers, and specialists involved in protecting children's well-being. In the context of these challenges, it is crucial to understand how interactions in the virtual environment affect the psychological development of children and adolescents and how digital space can be shaped to make it safe and support healthy development.

According to classical psychological developmental theories, a well-developed young adult is characterised by cognitive maturity, emotional stability, and social competence. Following Jean Piaget's theory, such an individual has reached the stage of formal operational thinking, demonstrating abstract reasoning, hypothetical-deductive logic, and reflective judgment essential for independent decision-making and future planning¹. Psychosocially, in Erik Erikson's framework, this stage reflects the successful resolution of identity formation, enabling the young adult to maintain a stable sense of self and personal values while navigating intimate and professional relationships². From Lev Vygotsky's sociocultural perspective, the young adult engages in collaborative learning and interpersonal problem solving, recognising the role of culture and language in ongoing development³. Finally, Bowlby's attachment theory suggests that emotionally healthy young adults internalise secure attachment patterns, allowing emotional regulation, trust in relationships, and resilience in the face of stress⁴. Together, these dimensions may define normative psychological development as a holistic integration of thought, identity, and affective competence.

The aim of this work is to present current research on the benefits and risks of children and adolescents using various online platforms. Such an understanding is necessary not only to better adapt upbringing and educational practices to the realities of the digital world, but also to develop effective legal regulations that will protect young users against the potential negative effects of their online presence. Finally, the roles of parents, teachers, and legislators in building a safe online environment for children and young people were presented.

In this study, the age ranges most commonly used in the psychological and medical literature were used. However, it should be noted that these are approximate boundaries; the child's development is individual, and the transition between stages

1 Cerovac and Keane, 2025, p. 62.

2 Kesavelu, Sheela and Abraham, 2021, pp. 75–76.

3 Saracho, 2023, p. 20.

4 Baldwin, 2020, pp. 37–53.

is not always clear or simultaneous for all individuals. The table below lists the names used together with the corresponding age ranges, and a summary of the more important developmental characteristics of each period.

Table 1. Developmental stages from infancy to emerging adulthood. A summary of the major characteristics in specific areas: cognitive, emotional, and social⁵

Age group / developmental stage	Cognitive development	Emotional development	Social development
1–3 years (toddlerhood)	Rapid sensorimotor learning, emerging language skills	Basic emotion expression, early regulation skills	Attachment to caregivers, early imitation
3–5 years (preschool-aged)	Symbolic play, basic reasoning, vocabulary expansion	Understanding of basic emotions, beginning of self-concept	Peer interactions, cooperative play begins
6–8 years (early school-aged)	Foundational literacy and numeracy, attention, and memory growth	Greater emotional control, development of self-esteem	Friendships based on shared activities, rule-following
9–11 years (middle childhood)	Concrete logical thinking, improved academic skills	Awareness of complex emotions, emotional empathy	Peer group importance increases, teamwork skills
12–14 years (early adolescence)	Abstract thinking, metacognition begins	Identity exploration, emotional sensitivity	Desire for peer approval, exploration of social roles
15–17 years (middle adolescence)	Critical thinking, complex problem-solving	Increased self-awareness, mood fluctuations	Deepening relationships, interest in romantic partnerships
18+ years (late adolescence / emerging adulthood)	Autonomous decision-making, long-term planning	Emotional stability, self-acceptance	Formation of lasting relationships, social responsibility

2. Children and Adolescents on the Internet

When starting to analyse the impact of online platforms on children's development, let us start by looking at the -Internet use habits of young people. It is worth paying attention to the results of the research conducted as part of the EU Kids Online project⁶, which covers 19 member states of the European Union. This study, which involved 25,101 people aged 9-17, provides valuable information and conclusions about the digital practices of young users.

This analysis reveals, without surprise, that the dominant device used for accessing the network among the surveyed group is a smartphone. In 11 countries - Croatia, the Czech Republic, Germany, Estonia, Italy, Lithuania, Norway, Poland, Portugal, Romania, and Serbia – the percentage of people aged 9-17 using mobile devices daily exceeds 80%. By contrast, laptops and desktop computers are used much less daily, with the lowest percentage of users (26%) in Switzerland and the highest (66%) in Lithuania. Mobile phones have a clear advantage over computers, with percentage

⁵ Source: Author's own elaboration.

⁶ Smahel et al., 2020, pp. 6–7.

differences ranging from 19% to 47%. In nine countries this difference exceeds 40%. Tablets, another device used to connect to the Internet, have varying degrees of popularity in everyday use, from 14% in Poland to 43% in Malta, with less than 25% using them daily in most European Union countries. In some countries, smart TV is more popular than tablets. Spain is at the forefront here, with almost 75% connecting to the Internet every day via TV. Italy is at the other extreme: only 17% use this method of accessing the Internet. Game consoles also vary in terms of daily use, ranging from 5% in Slovakia to 34% in Malta.

In summary, despite differences between countries in terms of preferred devices for Internet access, a significant proportion of young users use these devices daily. These results highlight the significant role digital devices play in the everyday lives of children and young people, constituting an essential element of their social interactions and access to information. The estimated daily time spent by children in the digital world ranges from 134 to 219 minutes in Switzerland and Norway, respectively. The report provides a lot of detailed information; however, here, let us take a closer look at the issue of differences between the sexes and between younger children and teenagers in the use of the most popular means, i.e., the smartphone.

The extent of children's daily Internet use on smartphones ranges from 35% to 68% in the case of boys and from 42% to 75% in the case of girls. In countries such as Estonia, France, Malta, Norway, Poland, Portugal, Serbia, and Slovakia, girls are slightly more likely than boys to use the Internet on smartphones several times a day, with the percentage difference ranging from six points (Estonia) to eleven points (Malta). Although these differences are relatively small, they indicate that in most countries, both boys and girls use smartphones at similar levels.

Age differences are more pronounced. In each of the countries surveyed, older children are more likely than younger children to use the Internet on smartphones daily. There is a clear gap between the youngest and oldest age groups, with the average difference being forty-six percentage points. In the youngest age group (9–11 years), the percentage of children using the Internet on smartphones daily ranges from 14% in France to 56% in Lithuania. However, in most countries, less than one-third of children in this age group use the Internet on a smartphone several times a day. For the 12–14 age group, the range of intensive use of the Internet on a smartphone range from 42% (Slovakia) to 84% (Norway). However, in the 15–16 age group, frequent use of the Internet on smartphones is much more common, with percentages ranging from 56% in Slovakia to 93% in Norway. In Switzerland and Spain, the difference between the youngest and oldest age groups is noticeable, reaching 69 and 62 percentage points, respectively. In contrast, in Lithuania, Croatia, and Slovakia, the difference is thirty-five percentage points or less, highlighting that older children are much more likely to use the internet on smartphones than younger children.

Now that we have an idea of how children gain access to the Internet, we must answer the question of what they do on-line. The activities that the authors of the project looked at were watching video clips, listening to music, communicating with family or friends, visiting a social networking, playing online games, using the

Internet for school purposes, browsing for things to buy, or checking their price, and searching for news. The extent of children's online activity shows significant differences between countries. Watching movies online ranges between 43% and 82%, with the lowest percentage in Slovakia and the highest in Lithuania. Similarly, the percentage of children listening to music on the Internet ranges from 45% in Germany to 81% in Serbia. Using the internet to communicate with friends and family shows an even wider range - from 14% in Germany to 77% in Romania, while visiting social networking sites ranges from 38% in Spain to 73% in Serbia. Online games enjoy varying levels of interest, from 27% of children playing them every day in Slovakia to 71% in Lithuania. Internet use for educational purposes also varies, with percentages ranging from 16% in Poland to 46% in Lithuania. In contrast, online shopping or browsing the Internet to check product prices is less popular, with the lowest percentage in Germany (8%) and the highest in Romania (41%). Finally, Internet use for reading or watching news ranges from 9% in Germany to 39% in Lithuania, showing that young Internet users engage in a wide range of digital activities with varying degrees of frequency depending on the country.

These data provide an overall picture of the digital engagement of children and young people. It should be noted that these data are from before the COVID-19 pandemic and before the restrictions introduced in many countries forced greater activity in the digital world. Many studies have demonstrated lifestyle changes and a significant increase in the online presence of children and adolescents during the pandemic⁷. However, we must wait for the results of systemic analyses to determine the durability of these changes after the end of the pandemic. However, we can confidently assume that the activity of children and young people on the Internet will not be lower than before the pandemic.

Which applications and online services do children use most often? There is a lack of analyses that collect such data from EU countries in one place. As the authors of the EU Kids Online project⁸ also point out, it is not always possible to obtain such data, and they may be incomplete. For example, popular applications are publicly available, and unless the user is logged in, it is impossible to say anything about them. Another problem is the issue of verifying the age of users; in many cases, this is limited only to the user's declaration that he is over 18 years of age or that he has his legal guardians' consent to use the website. Another problem is the issue of limiting some platforms to users over a certain age, for example, 13 years. Therefore, younger people theoretically have no right to use them, but verifying this is not always effective. Despite these limitations, some countries conduct research on the use of specific applications by children and adolescents. For example, Qustodio Technologies S.L. publishes annual reports on children and adolescents spending time on phones. The 2022 report⁹, based

7 Ie. Bates et al., 2020, p. 7; Xiang, Zhang and Kuwahara, 2020, p. 531; Rossi, Behme and Breuer, 2021, pp. 6–8; Singh and Balhara, 2021, p. 194; Vejmelka and Matković, 2021, pp. 11–15; Kamaşak et al., 2022, pp. 197–203.

8 Smahel et al., 2020, pp. 16–17.

9 Qustodio Technologies, 2023, p. 37.

on data from over 400,000 young users from the UK, US, Australia, and Spain, shows that children spend an average of four hours a day in front of personal device screens outside of school. On average, they spent most of their time playing Roblox, approximately three hours a day. They spend an average of 1 hour and 47 minutes watching short videos on TikTok and 1 hour and 07 minutes watching longer videos on YouTube, respectively. The Snapchat application is popular among Australian children and is used for an average of 1 hour and 14 minutes a day. For comparison, Spanish children spend 29 minutes a day outside of school on Smartick, a vocabulary and math learning app. Of course, the use of individual applications will vary among EU countries, and comparisons will often be difficult. Therefore, in the following section, we will focus not on individual websites but on the reasons why children and young people use them, as described in the first part of this subchapter.

3. Positive Impacts of Online Platforms

A review of the available scientific research on the impact of online platforms on the development of children and adolescents shows that scientists more often focus on the negative aspects of young people's Internet use. Another important observation is that analyses often separate the impacts of online games, learning platforms, and social media on younger users' psyches¹⁰. The same applies to research devoted to the positive aspects of the development of children and adolescents. The scientific literature most often distinguishes between three primary areas in which positive effects are observed: cognitive¹¹, psychosocial¹², and emotional development¹³, with the most positive changes observed in the cognitive area concerning knowledge and skills.

Research on cognitive development mainly concerns learning, memory, decision making, and logical thinking. The authors of the research indicate that the use of various applications for learning increases the efficiency and speed of acquiring new knowledge or learning a foreign language. Developing decision-making and logical thinking competencies is most often associated with playing online games. For example, a study by Agne Suziedelyte¹⁴ found that playing video games had a positive effect on children's problem-solving skills, while showing no significant impact on their reading skills. In turn, the work of Rusyaizil Ramla and Kristo Radion Purba¹⁵ focuses on the development of a game designed for Cognitive Therapy (CRT) aimed at improving attention span, memory, and problem-solving skills in children with learning disabilities. Nevertheless, other researchers believe that although the data indicate a certain development of cognitive processes under the influence of online

10 Underwood, George and Burnell, 2023, pp. 311–313.

11 Ramli and Purba, 2023, pp. 1–3.

12 Ross et al., 2021, pp. 299–300.

13 David, Predatu and Cardoso, 2018, pp. 57–60.

14 Suziedelyte, 2012, pp. 35–37.

15 Ramli and Purba, 2023, pp. 1–3.

platforms, this cannot be said unambiguously; more research is needed, especially experimental research, thanks to which it will be possible to clearly confirm the cause-and-effect relationship¹⁶. In addition, the use of various social media platforms can help children gain knowledge and education. Social media can serve as a source of knowledge and inspiration in many areas, offering young people access to educational materials, guides, and content that can expand their horizons and support the development of their interests and skills.

Some researchers¹⁷ highlight the positive impact of online platforms in the context of psychosocial development. Considering that communication between peers is increasingly moving to the Internet, it is not surprising that this aspect is gaining importance. Children and adolescents who have difficulty communicating in the real world (e.g., due to shyness or lack of skills) can acquire certain communication competences in the virtual world. They can also strengthen their self-esteem or self-confidence online, which may make it easier for them to function in life. Some authors suggest that online games can have a positive impact on users' socio-emotional development while highlighting the need for further research to delve deeper into these relationships. Therefore, the key in the educational context is the balanced use of online games, which considers the potential benefits and risks associated with their abuse or inappropriate use. Many online games promote cooperation and teamwork to achieve goals, which can help develop skills such as negotiation, communication and interpersonal interaction that are essential in everyday life. As a result, children learn effective cooperation, task division, and conflict resolution within a group. Online games also provide opportunities to build and maintain relationships. Through interactions in games, chats, and forums, young people can contact peers with similar interests from around the world, supporting the development of empathy, understanding cultural diversity, and creating lasting social bonds. Multiplayer games often require players to communicate and coordinate effectively, which helps them develop the ability to express their thoughts and needs clearly. Children learn to convey information, listen actively, and use specific game language and symbols to cooperate. Games can also support emotional development by allowing players to identify with the characters and share their experiences. This experience can lead to a better understanding of others' emotions, developing empathy, and the ability to feel and express their own emotions. In addition, the development of communication skills and building relationships can be supported using social media. They enable children and young people to easily communicate with their peers, which can support the building and maintenance of social relationships. For some young people, especially those who are shy or have difficulty making connections in the real world, social media can be a valuable tool for expressing themselves and

16 Mills, 2016, pp. 9–10.

17 Suziedelyte, 2012, pp. 35–37.

making friends. They also make it easier to find people with similar interests, which can encourage social interactions¹⁸.

When we look at the last area, i.e., emotional, researchers basically focus their attention on the supporting role of online platforms in cases of smaller or larger developmental deficits or situational difficulties¹⁹. It is worth noting that online interventions, such as group sessions with psychological and physical elements, can effectively reduce symptoms of anxiety and depression among children and adolescents, which was particularly evident during the COVID-19 pandemic²⁰. Another important aspect is support for children with developmental disorders. Online platforms can offer psychosocial services that support the emotional and behavioural well-being of homeschooled children, which are extremely important for, for example, people with autism²¹.

Table 2. A summary of the potential positive aspects of using online platforms²²

Age group / developmental stage	Cognitive	Emotional	Social
1–3 years (toddlerhood)	Simple sensory-motor apps support attention and hand-eye coordination.	Personalized videos provide comfort and routine.	Co-viewing with parents supports bonding.
3–5 years (preschool-aged)	Educational games teach letters, colours, shapes, and counting.	Apps teach emotion recognition and regulation.	Interactive platforms introduce collaboration.
6–8 years (early school-aged)	Logic and language games enhance reasoning and literacy skills.	Creative expression through digital art and stories.	Controlled platforms teach empathy and communication.
9–11 years (middle childhood)	Search tools and strategy games develop information processing.	Achievement systems support motivation and self-esteem.	Team games and chats improve peer interactions.
12–14 years (early adolescence)	Tools for self-directed learning and project work.	Exploration of identity and interests via social media.	Peer bonding and online support networks.
15–17 years (middle adolescence)	Growth of critical thinking and content creation skills.	Emotional awareness via expressive media (photography, writing).	Online civic engagement and youth participation.
18+ years (late adolescence / emerging adulthood)	Use of digital tools for academic and professional development.	Use of mindfulness and self-help platforms.	Building professional networks and collaboration skills.

4. Negative Impacts of Online Platforms

Researchers pay much more attention to the negative consequences of using online platforms. What could be causing these problems? To simplify, on the one hand, extremely progressive technological development and a lack of equally rapidly

18 Underwood, George and Burnell, 2023, pp. 309–312.

19 Bates, Greene and O’Quinn, 2021, pp. 443–447; Nasith, Bashith, 2023, pp. 699–700.

20 Wendel et al., 2023, pp. 3720–3723.

21 Nasith and Bashith, 2023, pp. 699–700.

22 Source: Author’s own elaboration.

developing regulations. On the other hand, there is a lack of sufficient digital education among both children and their parents. Children are often unaware of the consequences of their actions online, and parents may not understand how to protect their children from threats that await them. The impact of online platforms on children's development is a multidimensional phenomenon that includes psychological, social, and physical effects.

Psychological problems and related negative phenomena are more widely described in the literature than positive ones²³. Long-term Internet use can lead to cognitive problems, such as shortened attention spans in children, where instant gratification and the dynamic nature of digital content make it difficult or even impossible to engage in longer offline tasks or activities. Emerging research indicates that dopamine plays a significant role in the maladaptive use of online platforms by reinforcing repetitive engagement through reward-related neurobiological pathways. Like substance-based addictions, platforms such as social media and video-sharing sites activate dopaminergic circuits associated with gratification, especially in response to likes, notifications, and novel content stimuli²⁴. Chronic overstimulation of these pathways may lead to neuroplastic changes, including reduced dopamine receptor sensitivity, thereby increasing compulsive behaviours and tolerance²⁵. Behavioural addiction models emphasise the formation of feedback-driven habit loops, with dopamine acting as the key neurochemical mediator, even in the absence of physical withdrawal symptoms²⁶. Digital environments may also be intentionally designed to maximise user retention through dopaminergic feedback mechanisms, leading to sustained and often unconscious reengagement²⁷.

Moreover, regular exposure to online content can be a source of emotional disorders such as anxiety, depression, and low self-esteem, especially when young users compare themselves with idealised images from social media. Online platforms, particularly games and social media, can lead to compulsive use or addiction, whereby a child becomes overly dependent on these tools. Internet overuse can also interfere with homework and academic performance by eating up educational time or distracting students from academic activities. Additionally, long-term exposure to a variety of online content that may conflict with family values can affect a child's understanding of the concepts of right and wrong, creating confusion regarding morality. Children may also not be fully aware of privacy risks or dangerous online situations, which makes them vulnerable to cyberbullying and exposure to inappropriate content. Problems in the social area include limited development of social skills, making it difficult for children to interact face-to-face and understand nonverbal signals. This can lead to social isolation. Another problem can be caused by exposure to violent or inappropriate content. This may increase aggression (e.g., cyberbullying) or other

23 I.e. Kuss et al., 2014, pp. 4026–4052; Stoilova, Livingstone and Khazbak, 2021, pp. 12–13.

24 Macit, Macit and Güngör, 2018, p. 894.

25 Dresp-Langley and Hutt, 2022, p. 12.

26 Poisson, Engel and Saunders, 2021, pp. 3–9.

27 Eskandar, 2025, p. 18.

behavioural problems. In terms of negative effects on physical health, too much Internet use can cause eye strain, postural problems, sleep disturbances and an increased risk of obesity.

It should be noted that these problems often coexist. They rarely occur in isolation. For example, a person addicted to the Internet may experience social isolation as well as negative effects on physical health. Let us take a closer look at some of the most common problems: addiction, exposure to inappropriate content (including cyberbullying), social isolation, and sleep rhythm disturbances. Each of these phenomena can be attributed to a separate monograph, owing to their level of complexity. Therefore, we can provide only summaries here.

It is truistic to say that young people use the Internet and online platforms very often. Eurostat²⁸ data shows that, on average, 96% of young people in EU countries use the Internet daily. Does this mean that this percentage of people are addicted? Not necessarily. Internet addiction, also known as pathological Internet use or Internet use disorder, is defined as excessive or uncontrolled Internet use that negatively affects the user's daily life. Although not officially recognised as a diagnosable mental disorder by major diagnostic classifications such as DSM-5 (Diagnostic and Statistical Manual of Mental Disorders, 5th Edition)²⁹ and ICD-11 (International Classification of Diseases, 11th Revision)³⁰, it is nonetheless the subject of much research. Internet addiction may also include specific behaviours such as addiction to computer games, social media, use of dating sites, obsessive information tracking, or excessive online shopping. Internet addiction can be characterised by several basic features: spending too much time on the Internet (a person spends significantly more time online than necessary, often at the expense of important life activities, such as work, study, interpersonal relationships, or free time); increasing need to use the Internet (a person must spend more time online to achieve the desired feeling of satisfaction or stimulation); repeatedly unsuccessful attempts to control, limit, or stop using the Internet (the person makes repeated unsuccessful attempts to reduce the time spent in front of the screen or control the types of online activities); anxiety and nervousness when trying to limit Internet access (the person feels dysphoric, anxious, irritable, or nervous when trying to limit Internet use); neglect of other areas of life (excessive use of the Internet leads to the neglect of professional, educational, social, or parental duties); continuing excessive Internet use despite being aware of its negative consequences (this includes relationship problems, professional problems, and deteriorating physical and mental health); using the Internet to deal with negative emotions (a person may use the Internet to avoid personal problems or relieve mood states such as depression or anxiety).

28 Eurostat, 2024.

29 American Psychiatric Association, 2013. In DSM 5 Internet Gaming Disorder (IGD) is included in the III section. This means there should be more clinical research and experience, before IGD can be considered for as a formal disorder.

30 WHO, 2019a. In ICD-11 we have only code "6C51.0 Gaming disorder, predominantly online" and code "6C5Z Disorders due to addictive behaviours, unspecified".

As the Internet is ubiquitous and plays a significant role in everyday life, the diagnosis and treatment of Internet addiction can be quite complex and requires an individualistic approach.

Another frequent problem is the exposure to inappropriate content. The current digital landscape has radically changed the way children and young people experience the world. The Internet offers a huge reservoir of knowledge, educational tools, and social opportunities, but the same resources that can enrich, unfortunately carry serious risks related to the exposure of young users to inappropriate and even harmful content, from cyberbullying and pornography to content that promotes extreme behaviour or dangerous challenges. Children at an early age, not realising the consequences, share their personal data or photos on the Internet. Such behaviour may lead not only to immediate threats in the form of cyberbullying but also result in long-term problems such as identity theft or stalking.

Cyberbullying is a phenomenon most often defined as any behaviour by individuals or groups via electronic or digital media that repeatedly transmits hostile or aggressive messages intended to cause harm or discomfort to others³¹. Researchers also study the phenomenon of cybervictimization, which they define as exposing a person or group to harmful behaviour via information and communication technologies. Thus, a cyberbully is a person who abuses victims using technology, while a cybervictim is described as a person harmed by cyberbullying³². This distinction allows research to focus on the victim (what are the negative consequences of experiencing violence, and are there any variables/features that make it easier to become a victim?), the perpetrator (who and what is the perpetrator of violence? Why does he use violence? What negative consequences does he suffer from due to the use of violence?), or both sides of the violent phenomenon. Violent behaviour online includes, for example, hacking, sharing obscene photos (which, in the case of children and minors, is punishable by law in many countries), bullying, and stalking/trespassing. Research findings suggest that cyberbullying victimisation is strongly associated with psychological distress in most adolescents³³. Unfortunately, individual studies can only provide limited answers about who the victim/perpetrator of violence is and why it occurs; most often, it depends on specific research conducted in a specific environment and culture and considering a specific range of violent behaviours. Meta-analyses show certain trends, but most often, the effects are very low. However, one theme that often appears in the research is the role of support and communication with parents in overcoming the negative effects of violence.

The negative effects of experiencing violence, most often mentioned in the literature, may range from serious mental health problems such as anxiety, depression, or post-traumatic stress, to emotional disorders including feelings of fear, anger,

31 Farrington et al., 2023, pp. 9–10.

32 Akarsu, Budak and Okanlı, 2022, pp. 184–186.

33 Akarsu, Budak and Okanlı, 2022, pp. 184–186; Farrington et al., 2023, pp. 9–10; Griffith, Tetzlaff-Bemiller and Hunter, 2023, p. 7.

sadness, as well as a sense of powerlessness and isolation. Additionally, victims of cyberbullying often struggle with sleep disorders, including insomnia and nightmares, which negatively affects their overall health. Online bullying can also make it difficult to concentrate and learn, negatively affecting school performance and students' ability to focus on learning tasks. In extreme cases, people experiencing cyberbullying may engage in self-destructive behaviours, including suicidal thoughts or self-harm, as a way of coping with the emotional pain. Some victims may develop eating disorders that serve as unhealthy coping mechanisms for stress and negative emotions. Cyberbullying can also make it difficult to form and maintain healthy social relationships, both online and in the real world, due to the traumatic experience. Furthermore, the digital nature of this phenomenon allows for the easy review and dissemination of harmful content, which can lead to ongoing traumatising of the victim. Consequently, the quality of life of people experiencing cyberbullying can decrease significantly, thereby affecting their daily functioning, sense of security, and overall well-being. Additionally, victims of cyberbullying may encounter difficulties asserting their rights in the digital environment, which may result in a sense of injustice and frustration. Therefore, it is crucial to take preventive actions, including education and building awareness about the seriousness and consequences of cyberbullying as well as developing effective support tools for people who fall victim to cyberbullying.

Social isolation is another negative and dangerous phenomenon that may occur in young people because of Internet use. Generally, social isolation refers to a lack of relationships, little or no social support from others, or a lack of interpersonal contacts³⁴. However, this phenomenon may (but does not have to!) be related to loneliness (some researchers distinguish loneliness from the feeling of loneliness). It is an emotional state characterised by feelings of isolation or a lack of connection with other people. It is expressed through a lack of meaningful, close relationships, or a sense of belonging to a group. It is a disproportion between the current state of a person's social relations and the person's aspirations in this area. This may indicate that even an individual surrounded by many friends may experience loneliness. In the case of children and adolescents, among the sources of social isolation caused using online platforms, researchers most often mention excessive exposure to digital media³⁵, preferences for virtual interactions or their substitution with real ones³⁶, and the already mentioned online violence. Children and adolescents staying socially isolated may lead to many negative consequences on their mental and emotional health, social development, as well as physical health. Long-term social isolation is associated with a higher risk of developing depression, anxiety, and even personality disorders. Isolated people often experience deep states of sadness, hopelessness, and a lack of support, which may lead these disorders worsening. The feeling of loneliness, which is the subjective

34 CDC, 2024.

35 Tomoniko, 2019, pp. 4–9.

36 Anthony et al., 2023, pp. 7–9; Karapetyan and Gardner, 2023, pp. 76–78.

feeling of a lack of desired forms of social contact, also increases. This may lead to a negative impact on well-being and quality of life. Social isolation can lead to lower self-esteem because children and adolescents may interpret the reason for isolation as their own failures or lack of social acceptance. In terms of social effects, a lack of regular interaction with others can lead to a gradual weakening of social skills, such as communication, empathy, and conflict resolution. Isolation may building and maintaining close relationships difficult, which may lead to further withdrawal from social life.

The last area we will highlight here is the changes in sleep. The role of rest in physical and mental health is now obvious³⁷. Simultaneously, the role of sleep in the proper mental development of children and adolescents is clear³⁸. Many studies demonstrate that the length of sleep or its quality decreases in children and adolescents who spend time online³⁹. Therefore, incorrect use of online platforms by children and adolescents may lead to sleep disorders, which may negatively affect their mental and physical development. Poor sleep quality can lead to mental health problems such as depression, anxiety, and an increased risk of mood disorders. Sleep deficiency affects emotion regulation, which may worsen mental well-being and increase susceptibility to stress. Sleep disorders can negatively affect cognitive functions such as concentration, memory, and learning ability. Children and adolescents who suffer from sleep deprivation may have difficulty maintaining attention in school, which affects their academic performance and educational achievements. Sleep deprivation can lead to behavioural problems including impulsivity, aggression, and emotional control problems. Children and young people may have difficulty dealing with frustration and may be more likely to display negative behaviours. Sleep disorders can also affect physical health, increasing the risk of obesity, type 2 diabetes, and cardiac problems. Sleep deprivation affects the hormones that regulate appetite, which can lead to unhealthy eating habits and weight gain. Excessive use of online platforms can lead to the above-mentioned addiction to the Internet or games, which, in turn, can worsen sleep problems. This means that sleep disorders may both be a cause and a result of excessive use of digital media. Sleep disorders can affect social and familial relationships. Children and adolescents with sleep problems may be more irritable and less likely to participate in family and social activities. Fatigue resulting from sleep disturbances can increase the risk of accidents and injuries, both in and outside of school.

In conclusion, we must emphasise once again that the use of online platforms by children and adolescents may bring them benefits but may also be dangerous to their development. However, it is difficult to consider these issues separately because the processes that occur when using the Internet are complex and interconnected.

37 Muzni et al., 2021, pp. 10–12.

38 Lustig, Cote and Willoughby, 2021, pp. 6–9; Dutil et al., 2022, pp. 165–166.

39 Restrepo et al., 2020, pp. 6–8; Kokka et al., 2021, pp. 8–12; Ahmed et al., 2022 pp. 7–9; Gundogdu and Eroglu, 2022, pp. 690–692.

Negative effects may be both the cause and the effect of other unfavourable phenomena. Additionally, negative processes may go hand in hand with the benefits for children in other areas. The lines are incredibly thin; therefore, it is important to have a full picture of what is happening to your child when using online platforms.

Finally, it should be noted that an increasing number of studies indicate the negative consequences on mental health of using digital platforms too early in life. International guidelines consistently recommend limited and developmentally appropriate exposure to digital media in early childhood. According to the World Health Organization⁴⁰, screen time should be carefully regulated during early childhood to support optimal health and development. For infants under the age of one year, screen time is not recommended. One-year-old children should also avoid all screen exposure, while two-year-olds may be introduced to limited screen use not exceeding one hour per day, with shorter durations being preferred. For preschool-aged children between three and four years of age, screen time should be restricted to no more than one hour daily. Similarly, the American Academy of Paediatrics (AAP) recommends avoiding media use for children younger than 18 months (except for video chatting); introducing only supervised, high-quality content for toddlers aged 18–24 months; and limiting screen time to one hour per day for children aged 2–5 years⁴¹. The AAP emphasises the importance of consistent boundaries and media literacy education for school-aged children and adolescents. UNICEF focuses on ensuring that digital environments are age appropriate, inclusive, and safe, particularly regarding children's rights to privacy, protection, and equitable access⁴².

Studies highlight that early and excessive exposure to digital media in toddlerhood and preschool children may be a significant risk factor for the development of mental and behavioural disorders. Today, infants are exposed to screens as early as four months of age, and this early screen use has been linked to sleep disturbances and an increased risk of obesity, both of which are associated with emotional and cognitive regulation problems⁴³. Children with neurodevelopmental conditions such as autism spectrum disorder (ASD) appear particularly vulnerable to the overstimulation caused by digital environments, which can intensify the symptoms of social withdrawal and sensory overload⁴⁴. Cohort data from 12-month-olds also suggest that early screen exposure predicts longer screen times and possible behavioural problems in later childhood⁴⁵. Moreover, expert consensus highlights the association between high screen use and an increased risk of anxiety, depression, attention difficulties, and low self-esteem in young users⁴⁶.

40 WHO, 2019b, pp. 8–10.

41 Council on Communications and Media et al, 2016, p. 3.

42 WHO and UNICEF, 2022, p. 18.

43 Wolf et al., 2018, p. 4

44 Krishnan et al., 2021, p. 798.

45 Durham et al., 2021, pp. 7–8.

46 Anitha et al., 2021, pp. 269–279.

Table 3. A summary of the potential negative aspects of using online platforms⁴⁷

Age group / developmental stage	Cognitive	Emotional	Social
1–3 years (toddlerhood)	Delayed speech and attention from excessive screen time.	Sensory overload, irritability, dysregulation.	Limited caregiver interaction harms bonding.
3–5 years (preschool-aged)	Impaired problem-solving; reduced concentration.	Unrealistic emotional modelling by characters.	Poor sharing/cooperation if lacking offline play.
6–8 years (early school-aged)	Replacing active learning with passive content consumption.	Addiction to digital rewards (points, levels).	Isolation from real peers; facial cue misreading.
9–11 years (middle childhood)	Overstimulation hinders planning and retention.	Increased impulsivity and emotional reactivity.	Online-only relations may reduce empathy.
12–14 years (early adolescence)	Multitasking reduces academic performance.	Social comparison harms self-esteem and increases anxiety.	Cyberbullying and online peer rejection.
15–17 years (middle adolescence)	Difficulty focusing; information overload.	Increased risk of depression and anxiety.	Shallow relationships; face-to-face conflict avoidance.
18+ years (late adolescence / emerging adulthood)	Procrastination and reduced study/work motivation.	Dependency on digital coping mechanisms.	Weak offline relationship-building skills.

5. Implications for Parents, Educators, and Policymakers

It is an undeniable fact that the digital world is constantly evolving. Every few years, a significant step is taken in technological development, either at the level of hardware and access to it (constantly improving devices are available to an increasing percentage of the population) or software (development of the capabilities of various applications, the emergence of new ones, and the development of AI). Technology surrounds us and there is no sign that we will use it less. In contrast, the digital world makes our lives easier, supports work, and provides entertainment. We can expect future generations to use technology more often than earlier generations.

As stated previously, the issue of the impact of online platforms on the development of children and adolescents is multidimensional. It can bring a lot of good but also a lot of bad. Researchers show that regardless of whether we are parents, teachers, or professionals, we need to broadly understand education and the development of digital competence. We need knowledge of the current capabilities of various applications and tools on the Internet as well as the threats that lurk on the Internet. This knowledge must be constantly updated, because the digital world is changing rapidly. This is the first step toward ensuring the safe development of children and adolescents. The next steps will depend on the role we play.

Research shows the significant role of parents in counteracting or coping with the various negative consequences of dangerous phenomena. The most critical issue (although, in practice, it is often exceedingly difficult) is healthy communication. It is

47 Source: Author's own elaboration.

essential that parents talk to their children about their online experiences and that both parties communicate their concerns and feelings. Children should be encouraged to communicate honestly regarding what they find online. This helps build trust and openness in discussing potential problems. Simultaneously, this should be accompanied by setting boundaries. Parents should feel free to limit their children's screen time, especially before bedtime. Parents in cooperation with children, setting rules regarding the use of electronic devices, such as turning them off an hour before bed to support natural sleep patterns, is wise tactic. Content monitoring is an important aspect. Parents should be aware of the content that their children view or interact with online. Educational and constructive content that support cognitive and emotional development are worth promoting. Parents should be careful not to overcontrol their children as excessive control may have the opposite effect⁴⁸. Parents could encourage physical activity and support a healthy lifestyle. Regular physical activity and a suitable diet can improve sleep quality, reduce stress, and positively affect the psychophysical development of children and adolescents. Parents, particularly of younger children, have a decisive influence on digital education. Therefore, it is not only from them that the learning habits of using the Internet begins, but also the ability to manage time online, recognise and avoid cyberbullying, and protect privacy. It is also worth building good relationships between children and other young people by spending time together. Shared off-screen activities (board games, reading books, or outdoor activities) can not only strengthen family bonds and enable children to take a break from technology, but also build trust and space for healthy communication. It should also be noted that children, especially at the beginning of their development, learn everything from their parents (even if the parents are not aware of everything). Therefore, parents should consider how they use these online platforms. For example, should they not limit their own time spent on electronic devices, especially around children? Parents should develop healthy technology usage habits that can be passed on to their children.

Teachers, whether in kindergartens or schools, may also play a key role in supporting the healthy development of children and young people using online platforms. This is even more so when, in the education process, they increasingly use various applications for support and even conduct the entire remote education. Using technology in an educational manner can show students how to use online platforms for learning and development. These may include the use of educational applications, online collaboration tools, and digital resources to support the learning process. The primary areas that teachers can support are digital education and online safety. Teachers can incorporate lessons on staying safe online into their curricula, including topics such as data privacy, cyberbullying, and critical thinking about the information they find. Education in these areas will help students understand the risks associated with using the Internet and how to avoid them. Developing critical thinking can help address this issue. Teaching students how to evaluate information

48 Nguyen et al., 2022, pp. 7–9.

they find online is crucial in the age of fake news and disinformation. They should learn to verify sources, understand the differences between opinions and facts, and critically analyse digital content. Teachers should not forget to provide emotional and psychological support to those who experience negative effects of Internet use. Creating an atmosphere of openness in classrooms, where everyone can share their experiences and seek help, is important. Another area that teachers can help with is the development of soft skills such as communication, teamwork, and time management through group projects and tasks that require the use of technology. This will help students make better use of technology in their daily and professional lives. Educators can promote healthy digital habits, including a balance between online and offline lives. For example, they may demonstrate a need to take regular breaks from the screen, limit notifications, and use devices in a conscious and purposeful manner. At the same time, teachers should not forget about real life; they can encourage students to spend time offline, for example, practising sports, art, or developing their interests. Finally, it is important to remember that teachers cannot replace parents and should collaborate with them to promote healthy Internet habits at home. This may include organising information events and workshops, and providing educational materials to help parents understand how to support their children's healthy digital development.

Decision makers who shape the law also play a role in shaping the online environment for the safe development of children and youth⁴⁹. Policymakers can take several actions in this regard. The basic issue is support for research and development. This will facilitate diagnosing problem areas and planning and taking effective actions to support the safety and well-being of young Internet users. On the one hand, these activities may have an investment nature, supporting the creation of new, safe technologies. On the other hand, they may play a preventive and legislative role by creating and updating regulations aimed at counteracting cyberbullying, protecting personal data, and limiting access to harmful content. For example, content providers and online platforms can set requirements to filter and block inappropriate content for children. Some screen time regulations are possible, such as introducing maximum screen time recommendations for children and young people, and promoting apps and tools that help parents monitor and limit their children's digital device time. Policymakers can also develop and implement mechanisms to report abuse and harmful content online, and ensure that they are addressed quickly and effectively by online platforms and law enforcement agencies.

In addition to legislative activities, legislators usually have the proper tools to conduct large-scale educational and information activities, as well as social campaigns intended to increase public awareness of online safety, children's rights on the Internet, and methods of protection against digital threats. Digital education can be promoted by starting and supporting programs focused on the safe and conscious use of the Internet, critical online thinking, and digital skills, which are essential in

49 Fengchun et al., 2021, pp. 31–37.

today's world. It is also important to counteract digital exclusion. Policymakers can ensure that all students have equal access to digital resources and online education, which may include initiatives related to the availability of equipment and fast and secure Internet connections in homes and schools.

In summary, the safe development of children and adolescents using the Internet depends on what parents and teachers do and how legislators protect the online environment against undesirable phenomena. It should be remembered that parents and teachers can do the most at the early stages of the development of children and adolescents, which is why digital education should start from an early age at home, in kindergarten, and at school. Moreover, it should be constantly updated along with technological developments.

6. Summary

The impact of online platforms on the development of children and adolescents arouses many emotions and discussions among parents, teachers, and mental health and education specialists. There are an insufficient number of comprehensive publications in the literature on this subject that cover these phenomena comprehensively and use large samples. However, what is available provides some information about the nature of the phenomena in question and guidance on how to deal with them. The matter of research was complicated by the COVID-19 pandemic, which forced us to delve deeper into the digital world, contributing to the development of many platforms for communication, learning, and entertainment. In the era of digitisation and ubiquitous access to the Internet, online platforms have become an integral part of young people's everyday lives, offering them countless opportunities to gain experience, develop, and enjoy. However, apart from these benefits, there are challenges and potential risks that may affect their wellbeing and development.

On the one hand, the Internet is a rich source of knowledge and a tool that can significantly support the educational process. Access to teaching materials, online courses, and interactive educational applications enables children and young people to discover the world independently, develop passions, and acquire new skills. Moreover, social media platforms and communication applications make it easier to establish and maintain relationships with peers, which is crucial for social and emotional development. However, excessive Internet use and a lack of proper restrictions can lead to a number of negative consequences. Sleep disorders, Internet addiction, concentration problems, and cyberbullying are just some of the risks associated with the inappropriate use of online platforms. The issues of personal data security and privacy online are also important and require awareness and responsibility from young users.

Adults, parents, teachers, and legislators, play key roles in the face of these challenges. Through education, setting up clear rules for using the Internet, and promoting healthy digital habits, they can effectively support young people in safely

and constructively using online resources. It is also extremely important to build trust and open dialogues that will allow children and young people to express their concerns and problems related to life in the virtual world.

In summary, online platforms significantly impact the development of children and young people by offering both opportunities and challenges. The key to maximising benefits and minimising risks is the responsible use of the Internet supported by an aware and engaged adult environment. Thus, the digital world can become a safe and inspiring place for young users, supporting their comprehensive development.

Bibliography

- Ahmed, G.K., et al. (2022) 'Relationship between time spent playing internet gaming apps and behavioral problems, sleep problems, alexithymia, and emotion dysregulations in children: a multicentre study', *Child and Adolescent Psychiatry and Mental Health*, 16(67), pp. 1–11; <https://doi.org/10.1186/s13034-022-00502-w>.
- Akarsu, Ö., Budak, M.İ., Okanlı, A. (2022) 'The relationship of childhood trauma with cyberbullying and cyber victimization among university students', *Archives of Psychiatric Nursing*, 2022/41, pp. 181–187; <https://doi.org/10.1016/j.apnu.2022.06.004>.
- American Psychiatric Association (2013) *Diagnostic and statistical manual of mental disorders*. 5th edn. Virginia: American Psychiatric Association Publishing; <https://doi.org/10.1176/appi.books.9780890425596>.
- Anitha, F. S., et al. (2021) 'Association of digital media exposure and addiction with child development and behavior: A cross-sectional study'. *Industrial Psychiatry Journal*, 30(2), pp. 265–271; https://doi.org/10.4103/ipj.ipj_157_20.
- Anthony, R., et al. (2023) 'Young people's online communication and its association with mental well-being: results from the 2019 student health and well-being survey', *Child and Adolescent Mental Health*, 28(1), pp. 4–11; <https://doi.org/10.1111/camh.12610>.
- Baldwin, L. (2020) 'Cognitive and Emotional Development of Young People and the Development of Resilience' in Baldwin, L. (ed.) *Nursing Skills for Children and Young People's Mental Health*. Cham: Springer, pp. 37–53; https://doi.org/10.1007/978-3-030-18679-1_3.
- Bates, L.C., et al. (2020) 'COVID-19 Impact on Behaviors across the 24-Hour Day in Children and Adolescents: Physical Activity, Sedentary Behavior, and Sleep', *Children*, 7(9), 138; <https://doi.org/10.3390/children7090138>
- Bates, S., Greene, D., O'Quinn, L. (2021) 'Virtual Sport-Based Positive Youth Development During the COVID-19 Pandemic', *Child and Adolescent Social Work Journal*, 2021/38, pp. 437–448; <https://doi.org/10.1007/s10560-021-00774-9>.
- Cerovac, M., Keane, T. (2025) 'Early insights into Piaget's cognitive development model through the lens of the Technologies curriculum', *International Journal of Technology and Design Education*, 2025/35, pp. 61–81; <https://doi.org/10.1007/s10798-024-09906-5>.
- CDC (2024) 'Health Risks of Social Isolation and Loneliness', *cdc.gov*, 15 May [Online]. Available at: https://www.cdc.gov/social-connectedness/risk-factors/?CDC_AAref_Val=https://www.cdc.gov/emotional-wellbeing/social-connectedness/loneliness.html (Accessed: 9 April 2025).
- Council on Communications and Media, et al. (2016) 'Media and young minds', *Pediatrics*, 138(5), e20162591; <https://doi.org/10.1542/peds.2016-2591>.

- David, O.A., Predatu, R.M., Cardoso, R.A.I. (2018) 'A pilot study of the RETHink online video game applied for coaching emotional understanding in children and adolescents in the therapeutic video game environment: The feeling better resources game', *Journal of Evidence-Based Psychotherapies*, 18(1), pp. 57–68; <https://doi.org/10.24193/jebp.2018.1.5>.
- Dresp-Langley, B., Hutt, A. (2022) 'Digital Addiction and Sleep', *International Journal of Environmental Research and Public Health*, 19(11), 6910. <https://doi.org/10.3390/ijerph19116910>.
- Durham K, et al. (2021) 'Digital Media Exposure and Predictors for Screen Time in 12-Month-Old Children: A Cross-Sectional Analysis of Data From a German Birth Cohort', *Frontiers in Psychiatry*, 2021/12, 737178; <https://doi.org/10.3389/fpsyt.2021.737178>.
- Dutil, C., et al. (2022) 'Sleep timing and health indicators in children and adolescents: a systematic review', *Health Promotion and Chronic Disease Prevention in Canada: Research, Policy and Practice*, 42(4), pp. 150–169; <https://doi.org/10.24095/hpcdp.42.4.04>.
- Eskandar, K. (2025) 'The digital trap: unraveling the neuropsychological impact of technology addiction', *Neuropsychological Trends*, 2025/37, pp. 7–23; <https://doi.org/10.7358/neur-2025-037-eska>.
- Eurostat (2024) 'Individuals – frequency of internet use', *eurostat* [Online]. Available at: https://ec.europa.eu/eurostat/databrowser/view/ISOC_CI_IFP_FU__custom_6541841/bookmark/table?lang=en&bookmarkId=49d9ace1-03f3-4eb1-909b-09e67c2a5e1e (Accessed: 1 February 2024).
- Farrington, D.P., et al. (2023) 'Cyberbullying research in Canada: A systematic review of the first 100 empirical studies', *Aggression and Violent Behavior*, 2023/69, 101811; <https://doi.org/10.1016/j.avb.2022.101811>.
- Fengchun, M., et al. (2021) *AI and education: A guidance for policymakers*. Paris: UNESCO Publishing; <https://doi.org/10.54675/PCSP7350>.
- Griffith, C.E., Tetzlaff-Bemiller, M., Hunter, L.Y. (2023) 'Understanding the cyber-victimization of young people: A test of routine activities theory', *Telematics and Informatics Reports*, 2023/9, 100042; <https://doi.org/10.1016/j.teler.2023.100042>.
- Gundogdu, U., Eroglu, M. (2022) 'The relationship between dissociation symptoms, sleep disturbances, problematic internet use and online gaming in adolescents', *Psychology, Health and Medicine*, 27(3), pp. 686–697; <https://doi.org/10.1080/13548506.2021.1984542>.
- Kesavelu, D., Sheela, K., Abraham, P. (2021) 'Stages of psychological development of child-an overview', *International Journal of Current Research and Review*, 13(13), pp. 74–78; <http://dx.doi.org/10.31782/IJCRR.2021.131320>.
- Kuss, D. J., et al. (2014) 'Internet addiction: A systematic review of epidemiological research for the last decade', *Current pharmaceutical design*, 20(25), pp. 4026–4052; <https://doi.org/10.2174/13816128113199990617>.

- Kamaşak, T., et al. (2022) 'An Investigation of Changing Attitudes and Behaviors and Problematic Internet Use in Children Aged 8 to 17 Years During the COVID-19 Pandemic', *Clinical Pediatrics*, 61(2), pp. 194–205; <https://doi.org/10.1177/00099228211065842>.
- Karapetyan, A., Gardner, S. (2023) 'The Online and Offline Communication Preferences of Armenian Social Network Users', *Journal of Sociology: Bulletin of Yerevan University*, 14(2 (38)), pp. 66–80; <https://doi.org/10.46991/BYSU:F/2023.14.2.066>.
- Kokka, I., et al. (2021) 'Exploring the Effects of Problematic Internet Use on Adolescent Sleep: A Systematic Review', *International Journal of Environmental Research and Public Health*, 18(2), 760; <https://doi.org/10.3390/ijerph18020760>.
- Krishnan, V., et al. (2021) 'Early Social Experience and Digital-Media Exposure in Children with Autism Spectrum Disorder', *Indian Journal of Pediatrics*, 2021/88, pp. 793–799; <https://doi.org/10.1007/s12098-021-03666-z>.
- Lustig, K.A., Cote, K.A., Willoughby, T. (2021) 'The role of pubertal status and sleep satisfaction in emotion reactivity and regulation in children and adolescents', *SLEEP Advances*, 2(1), zpab003; <https://doi.org/10.1093/sleepadvances/zpab003>.
- Macit, H. B., Macit, G., Güngör, O. (2018) 'A research on social media addiction and dopamine driven feedback', *Journal of Mehmet Akif Ersoy University Economics and Administrative Sciences Faculty*, 5(3), pp. 882–897; <https://doi.org/10.30798/makuiibf.435845>.
- Mills, K.L. (2016) 'Possible Effects of Internet Use on Cognitive Development in Adolescence', *Media and Communication*, 4(3), pp. 4–12; <https://doi.org/10.17645/mac.v4i3.516>.
- Muzni, K., et al. (2021) 'Self-reported sleep quality is more closely associated with mental and physical health than chronotype and sleep duration in young adults: A multi-instrument analysis', *Journal of Sleep Research*, 30(1), e13152; <https://doi.org/10.1111/jsr.13152>.
- Nasith, A., Bashith, A. (2023) 'The Optimization of Children's Autism Psychosocial Service on Online School Learning', *Scaffolding: Journal Pendidikan Islam dan Multikulturalisme*, 5(2), pp. 685–702; <https://doi.org/10.37680/scaffolding.v5i2.2371>.
- Nguyen, T.T.P., et al. (2022) 'Parent–Child Relationship Quality and Internet Use in a Developing Country: Adolescents' Perspectives', *Frontiers in Psychology*, 2022/13, <https://doi.org/10.3389/fpsyg.2022.847278>
- Poisson, C.L., Engel, L., Saunders, B.T. (2021) 'Dopamine Circuit Mechanisms of Addiction-Like Behaviors', *Frontiers in Neural Circuits*, 2021/15, 752420; <https://doi.org/10.3389/fncir.2021.752420>.
- Qustodio Technologies (2023) 'Qustodio releases 2022 Annual Report, From Alpha to Z: Raising the digital generations', *qustodio.com*, 7 February [Online]. Available at: <https://www.qustodio.com/en/research/qustodio-releases-2022-annual-report/> (Accessed: 9 January 2024).

- Ramli, R., Purba, K.R. (2023) 'The development of a Game for Cognitive Remediation Therapy (CRT) to Improve Attention Span and Memory Among Children with Learning Disabilities' in IEEE (ed.) *2023 19th IEEE International Colloquium on Signal Processing and Its Applications (CSPA)*. Piscatawa: IEEE, pp. 1–6; <https://doi.org/10.1109/CSPA57446.2023.10087548>.
- Restrepo, A., et al. (2020) 'Problematic internet use in children and adolescents: associations with psychiatric disorders and impairment', *BMC Psychiatry*, 2020/20, 252; <https://doi.org/10.1186/s12888-020-02640-x>.
- Ross, A.C., et al. (2021) 'Associations Between Off-line Social Functioning and Online Social Network Interactions Among Emerging Adults', *Emerging Adulthood*, 9(4), pp. 292–304; <https://doi.org/10.1177/2167696820905179>.
- Rossi, L., Behme, N., Breuer, C. (2021) 'Physical Activity of Children and Adolescents during the COVID-19 Pandemic – A Scoping Review', *International Journal of Environmental Research and Public Health*, 18(21), 11440; <https://doi.org/10.3390/ijerph182111440>.
- Saracho, O.N. (2023) 'Theories of Child Development and Their Impact on Early Childhood Education and Care', *Early Childhood Education Journal*, 2023/51, pp. 15–30, <https://doi.org/10.1007/s10643-021-01271-5>.
- Singh, S., Balhara, Y.P.S. (2021) "Screen-time" for children and adolescents in COVID-19 times: Need to have the contextually informed perspective', *Indian Journal of Psychiatry*, 63(2), pp. 192–195; https://doi.org/10.4103/psychiatry.IndianJPsychiatry_646_20.
- Smahel, D., et al. (2020) *EU Kids Online 2020: Survey results from 19 countries*. London: The London School of Economics and Political Science; <https://doi.org/10.21953/lse.47fdeqj01ofo>.
- Stoilova, M., Livingstone, S., Khazbak, R. (2021) *Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes*. Innocenti Discussion Paper 2020-03. Florence: UNICEF Office of Research [Online]. Available at: <https://www.unapcict.org/sites/default/files/2021-03/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf> (Accessed: 13 February 2024).
- Suziedelyte, A. (2012) 'Can Video Games Affect Children's Cognitive and Non-Cognitive Skills?', *UNSW Australian School of Business Research Paper*, 2012/37; <http://dx.doi.org/10.2139/ssrn.2140983>
- Tomoniko, S. (2019) 'Anxiety at Teenagers' Fingertips', *BU Journal of Graduate Studies in Education*, 11(2), pp. 4–11.
- Underwood, M.K., George, M.J., Burnell, K. (2023) 'Socially networked lives: How adolescents and young adults engage with social media' in American Psychological association (ed.) *APA handbook of adolescent and young adult development*. Washington, DC: American Psychological Association, pp. 307–321; <https://doi.org/10.1037/0000298-019>.

- Vejmelka, L., Matković, R. (2021) 'Online Interactions and Problematic Internet Use of Croatian Students during the COVID-19 Pandemic', *Information*, 12(10), 399; <https://doi.org/10.3390/info12100399>.
- Wendel, F., et al. (2024) 'Interventions to build resilience and to ameliorate negative psychosocial effects of the COVID-19 pandemic on children and adolescents: a systematic review and meta-analysis', *European Child and Adolescent Psychiatry*, 2024/33, pp. 3707–3726; <https://doi.org/10.1007/s00787-023-02280-y>.
- Wolf, C., et al. (2018) 'Children's Environmental Health in the Digital Era: Understanding Early Screen Exposure as a Preventable Risk Factor for Obesity and sleep Disorders', *Children*, 5(2), 31; <https://doi.org/10.3390/children5020031>.
- WHO (2019a) 'Eleventh Revision of the International statistical Classification of Diseases and Related Health Problems (ICD-11)' [Online]. Available at: <https://icd.who.int/en/docs/icd11-license.pdf> (Accessed: 31 July 2025).
- WHO (2019b) *Guidelines on physical activity, sedentary behaviour and sleep for children under 5 years of age*. Geneva: World Health Organization.
- WHO, UNICEF (2022) *Nurturing care handbook. Strategic action 5: scale up and innovate. How to expand programmes, engage with the private sector and use digital solutions*. Geneva: World Health Organization and the United Nations Children's Fund (UNICEF).
- Xiang, M., Zhang, Z., Kuwahara, K. (2020) 'Impact of COVID-19 pandemic on children and adolescents' lifestyle behavior larger than expected', *Progress in Cardiovascular Diseases*, 63(4), pp. 531–532; <https://doi.org/10.1016/j.pcad.2020.04.013>.

Children in Digital Age – International Regulations

Sanja SAVČIĆ

ABSTRACT

The advent and rapid development of computer technology have revolutionised human society. In a remarkably short period, technology has transformed daily life, shifting from occasional computer use to the Internet as the primary channel of communication, and now to artificial intelligence, which enables machines to mimic human behaviour and decision-making. Historically, such profound changes took centuries; today, they are occurring at an unprecedented pace, leaving many struggling to adapt. While digitalisation has made technology more user-friendly and widely accessible across generations, disparities in digital skills persist. Younger generations often fully grasp the potential of digital technology, while their parents may lack equivalent expertise. This reality is creating a widening generational gap, even more pronounced than in previous decades. Children are particularly adept at using innovative technologies, especially the Internet, yet they may not fully understand the real-world consequences of their online activities. Conversely, parents are generally more aware of the associated risks and dangers, though they often lack the same technical proficiency. Growing up in a more traditional society, these older generations may feel somewhat constrained by the pervasive digitalisation of life. While they observe the process of digital integration, they do not always participate actively. From the perspective of children's rights, this new age poses challenges for scholars and legislatures alike. Although it is tempting to examine each right in isolation, certain rights are particularly difficult to enforce in the digital realm. This work will explore these rights in detail.

KEYWORDS

digital age, children's rights, right to privacy, right to education, right to be informed

1. Introduction

Children constitute 30% of the global population,¹ with figures as low as 10–15% per country in Europe. This highlights both their statistically weaker position and their vulnerability, given their limited mental and physical maturity. Historically, children have been especially disadvantaged due to certain natural, cultural, and political factors, often bearing the brunt of violent conflict and disease outbreaks.

| 1 Worldometers, n.d. |

| Sanja SAVČIĆ (2025) 'Children in Digital Age – International Regulations' in Halász, Cs. (ed.) (2025) *Children in Digital Age*. Miskolc–Budapest: Central European Academic Publishing, pp. 49–65. https://doi.org/10.71009/2025.csh.cida_3. |

The adoption of the United Nations Convention on the Rights of the Child (CRC) at the end of the last century dramatically transformed the status of children.² The CRC, the most comprehensive international legal instrument for children's rights, was prepared after ten years of intensive negotiations.³ Following numerous ratifications, the CRC has become one of the most significant human rights treaties. However, the true challenge for children's rights emerged after the CRC came into legal force, as its implementation at the national level needed to reflect the diverse social, cultural, religious, and economic contexts of the States Parties. Moreover, the years immediately following the CRC's adoption were marked by unprecedented technological advancements, particularly the impact of global networking on everyday life, which made this diversity even more evident. This raises the question of whether the CRC has the potential to continue shaping children's rights in the years ahead.⁴

The digital environment increasingly makes children's lives more virtual than real, as nearly every human activity can now be undertaken in a parallel digital world. Consequently, global society, which has not yet fully adapted children's rights to the circumstances that existed prior to the adoption of the CRC, now faces new challenges in the digital environment. To identify the weak points in the exercise and protection of children's rights, the CRC, as a key international regulatory instrument, must be analysed from a digital perspective.

2. The Digital World: What Has It Brought to Society?

The creation and development of computer technology heralded a revolution in human society. Within a short period, technology has repeatedly and profoundly transformed daily life: from the incidental use of computers, to the Internet becoming the dominant channel of communication, and finally to artificial intelligence, which enables machines to imitate human behaviour and decision-making. Historically, such dramatic sociocultural evolution took centuries, but today's rapid advancements are proving challenging to keep pace with. For example, a middle-aged woman today may still remember dial-up phones, black-and-white television, and short cartoons from her early childhood, followed later by the first friend or peer to own a mobile phone. From a technological perspective, the overarching process of digitalisation has made technology more user-friendly and thus widely accepted across all generations.

2 United Nations, 20 November 1989. In New York. After Somalia ratified the CRC, the USA remain the only United Nations member state that did not accept the CRC.

3 Skoler, 1993, p. 38.

4 The interests of child have been recognised in the United Nations Millenium Declaration, adopted on 8 September 2000. Six of the eight Millennium Development Goals protect the rights of children to health, education, Protection, and equality. They will only be sustained when the rights of every child are realised. These six goals also match the goals set out in "A World Fit for Children" (The Millenium Development Goals, 2003).

However, digital skills often vary by generation. The youngest generations frequently understand the full potential of digitalisation, while their parents may not, contributing to an increasing technological gap. Children are masters of innovative technology, especially the Internet, yet they remain unaware of its real-life consequences.⁵ In contrast, parents are more aware of these consequences and potential dangers, but they are not as technologically skilled as their children. Growing up in a more traditional society, these older generations may reject the unrestrained digitalisation of every aspect of life. They are witnesses to the process of digitalisation but are not necessarily active participants in it.

For these reasons, the Internet has become a central topic in both societal and legal discussions. Digitalisation has challenged not only technical and technological fields but also the social sciences. As for the law, especially children's rights, it is essential to understand exactly what digitalisation – particularly, the Internet – has changed in the traditional relationships of society.

3. Legal Framework: Challenges of Digitalisation

Among the many challenges of digitalisation, “communication” is a fundamental process in human civilisation and one that underpins all these challenges. Communication serves as a means of interaction and as a legal mechanism for a child to exercise their rights; however, it can also inadvertently infringe upon the rights of others. The digital environment has increased connectivity among children, making it an integral aspect of their lives and well-being. Modern technology enables children to create their own communities and share their views or daily experiences within these communities or on social networks.⁶ These realities render the digital environment vulnerable, as social networks lack age-specific restrictions. Children are exposed to the adult world, despite being ill-equipped to distinguish between the benefits and risks of such interactions. A significant obstacle to protecting children's rights in the digital world is that the prominent actors in the digital space are privately owned and largely self-regulate their activities. From a pragmatic perspective, this approach to shaping the virtual world is flexible, yet it underscores the need for legal certainty. Regarding children's rights, self-regulation circumvents the territorial constraints inherent in conventional jurisdictional frameworks, creating additional challenges in protecting children in the digital age.⁷

It is also important to note the dominant narrative in the mass media regarding the risks of Internet communication. These include cyberbullying, child trafficking on the dark web, the drug trade, access to graphic and explicit content, harmful impacts on teenagers' mental well-being and self-esteem, online harassment, and

5 Franco and Almog, 2019, pp. 75–78.

6 Papandrea, 2008, pp. 1032–1037.

7 Choudhuri, 2019, p. 153.

more.⁸ Understanding the comprehensive impact of digital technology on children's lives must also address "digital dependency," driven by the early use of smartphones and the increasing problem of smartphone addiction. A crucial question remains: can the pre-eminent international document, the CRC, be applied effectively in the digital world?⁹

4. The United Nations Convention on the Rights of the Child

Although the CRC is recognised as the cornerstone document on children's rights, it is not a perfect human rights treaty.¹⁰ Any assessment of the document's quality must consider the realistic expectations of its implementation. In this regard, the CRC does not provide strict rules and mechanisms that can be applied automatically, but instead sets out a series of principles that form a framework for the regulation of children's rights in line with the legal, social, religious, and cultural traditions of each State Party. These principles are rooted in key rights: the right to non-discrimination (Art. 2); the right to life, survival and development (Art. 6); the right to be heard (Art. 12); and the imperative to consider the best interests of the child in all activities (Art. 3). All other provisions should be interpreted in light of these core principles. These principles should guide authorities during the implementation process to achieve the goal of the CRC: enabling children to reach their full potential in the society to which they belong. The CRC defines a child for the purposes of this act and establishes a comprehensive range of children's rights (Part I). Some of these rights, such as the right to citizenship (Art. 7), are less relevant to the emerging digital world of children. Others, however, are particularly significant to contemporary discussions. The CRC applies to all individuals below the age of 18 (Art. 1), although if national law establishes majority at an earlier age, that national law is applied. Nevertheless, countries are obliged to protect children from all forms of discrimination and to take positive action to promote their rights. All actions concerning children must be guided by their best interests. States are obligated to ensure appropriate care when parents or guardians fail to do so, and to ensure the rights set out in the CRC are realised. Children must be consulted on the realisation of their rights, in accordance with their age and maturity.

The following rights are guaranteed to children: the right to life (Art. 6); to a name, to acquire a nationality, and to know and be cared for by his or her parents (Art. 7); to preserve identity, including nationality, name, and family relations (Art. 8); to live with their parents (Art. 9–11); to form and freely express their views (Art. 12); to freedom of expression (Art. 13); to freedom of thought, conscience, and religion (Art. 14); to freedom of association and peaceful assembly (Art. 15); to privacy (Art. 16); to

8 Ibid., p. 154.

9 Grover, 2004, pp. 269–270.

10 Savić, 2019, p. 303.

be appropriately informed (Art. 17); and to special protection in cases where there is no parental care, including adoption (Art. 20, 21).

Also guaranteed are the rights of refugee children or children seeking refugee status to special protection (Art. 22); the right of the disabled child to special care (Art. 23); the right to health and healthcare (Art. 24, 25); the right to social security, including social insurance (Art. 26); the right to an adequate standard of living (Art. 27); and the right to education (Art. 28, 29). Further rights include the protection of children belonging to minority groups (Art. 30); the right to rest and leisure, play and recreational activities, and participation in cultural life and the arts (Art. 31); protection from economic exploitation (Art. 32); protection from the misuse of harmful substances (Art. 33); protection from sexual exploitation, abduction and trafficking (Art. 34); protection from torture and deprivation of liberty (Art. 37); safeguarding children in armed conflicts (Art. 38); and the right to special juvenile justice (Art. 40).

Within Part I, the CRC also regulates the responsibility for the upbringing and development of the child, establishing the primary responsibility of parents or legal guardians in raising their children. However, the state's obligation to protect the child from all forms of abuse and neglect is also clearly defined, and includes both preventive programmes and support for victims of abuse. Given the vulnerability of children and the risk of physical, mental, and sexual abuse, respect for privacy and family life cannot take precedence when the vital interests of the child are endangered (Arts. 18, 19). This provision underscores the need to prioritise the child's well-being above privacy and family life when their safety is at risk. It highlights the vulnerabilities children face and the imperative to safeguard their rights and protection from harm, whether from third parties or from parents themselves.

5. Other International Regulations on Children's Rights

Armed conflicts have persisted even after the end of the Second World War and the institution of numerous peace treaties. Increasing numbers of people have become victims of armed conflicts, with children being the most vulnerable. With the adoption of the Rome Statute of the International Criminal Court, the recruitment or mobilisation of children under the age of 15 and the use of children for active participation in hostilities are classified as war crimes. At the 26th International Conference of the Red Cross and Red Crescent in December 1995, it was recommended that parties to conflicts take all measures to ensure that children under the age of 18 do not participate in hostilities. To protect children during armed conflicts, the United Nations adopted the Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflicts in 2000. The aim of this Protocol is to raise the age limit for the voluntary recruitment of individuals into state armed forces to 18 years.

For the protection of children in the digital world, the second Optional Protocol to the CRC is particularly relevant: the Optional Protocol to the Convention on the

Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. This Optional Protocol responds to the increased risk of sexual exploitation faced by children. In the era of the Internet, characterised by fast and borderless communication, the sexual abuse of children can take various forms across networking and communication channels. The Optional Protocol defines the sale of children, child prostitution and child pornography, and provides measures to combat these grave issues. The contracting states are obliged to fully criminalise these acts in their national laws, whether committed domestically, transnationally, individually, or on an organised basis. The states must implement laws and strengthen social policies and programmes to prevent the illegal actions covered under the Optional Protocol. They are also committed to raising public awareness through information, education and training. To achieve this, international cooperation is expected to be enhanced through multilateral, regional and bilateral agreements. The goal of the Optional Protocol is to elevate standards beyond those set in Article 34 of the CRC. Supervision of the Original Protocol's implementation, as with the CRC, is carried out by the Committee on the Rights of the Child, a body established to monitor the progress made by the contracting states in fulfilling their obligations.

Besides United Nations agreements, states are also actively engaged in intensive legislative activities. In the European context, the most relevant documents include the European Convention on Human Rights and Fundamental Freedoms (and its amending protocols) (ECHR), the European Convention on Cybercrime (Budapest Convention), and the European Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Although all these conventions were adopted by the Council of Europe and are therefore regional, their influence extends far beyond what is typically expected from regional documents.

The ECHR, adopted in 1950, was inspired by the Universal Declaration of Human Rights. Aiming to create a democratic world by promoting civil rights and freedoms, it did not explicitly regulate the position of children as a distinct category. However, its impact cannot be overstated, thanks to the case law of the European Court of Human Rights (ECtHR). The establishment of the ECtHR has contributed to citizens' trust in universal justice, ensuring the protection of their rights even against the state. Since the ECHR contains only a few explicit references to children's rights, the interpretation of the CRC by the ECtHR has significantly shaped the European approach to the protection of children's rights.

The Budapest Convention on Cybercrime is a legal response to the long-standing demand to combat cybercrime. It was adopted by the Council of Europe, which includes 47 member states in the European region, along with some non-member states, and it plays a significant role in establishing collective action towards the harmonised criminalisation of cybercrime and synchronised intervention. As the first binding multinational treaty addressing cybercrime, its provisions have been widely adopted across many countries. The most notable outcome of the Budapest Convention is the explicit criminalisation of cybercrime and the promotion of state collaboration in prosecuting offenders.

The investigation of transnational cybercrime requires the cooperation of law enforcement agencies across all relevant countries. The formal mechanisms for international cooperation in combating cybercrime include mutual legal assistance and extradition. Mutual assistance regarding provisional measures is particularly important, as it encompasses expedited preservation of stored computer data, expedited disclosure of preserved traffic data, access to stored computer data, and the real-time collection of computer data. In relation to cyberbullying, this cooperation is crucial in protecting children in the digital world.

The Lanzarote Convention is the first regional treaty specifically dedicated to the protection of children from sexual violence. Adopted in 2007 and entering into force in 2010, it has been signed by all Council of Europe member states. Together with the Budapest Convention, it forms an extensive framework for the protection of children in the digital space. As stated in the preamble of the Lanzarote Convention (para. 3), every child has the right to the protective measures required by their status as a minor, provided by their family, society and the state. The Lanzarote Convention adopts the so-called “4P approach” in protecting children’s sexual rights: prevention, protection, prosecution and promotion. This approach addresses all aspects of the growing issue of child abuse in the digital environment. By providing clear definitions of criminal acts against children and establishing a set of guidelines for implementation, the Lanzarote Convention affords a strong legal framework. It includes robust rules and procedures for the protection of victims, which are crucial for a child’s mental health and self-confidence. The impact of the Lanzarote Convention is further reinforced by expectations regarding international cooperation through the full implementation of its measures. Monitoring how state parties implement the Lanzarote Convention in legislation and policy is entrusted to the Committee of the Parties to this treaty, known as the Lanzarote Committee.

6. Key Rights of the Child in the Digital Age

Although it is challenging to consider each child’s rights in isolation from others, some rights may be more difficult to enforce in the digital space. These rights will be examined in detail.

6.1. *Right to Privacy*

Art. 16 of the CRC stipulates that no child shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honour and reputation. In the digital environment, children have the right to privacy and family life, which includes the protection of their personal data and the respect for the confidentiality of their private communications.¹¹

11 Council of Europe, 2018.

Although there is no universally accepted definition of privacy, its general meaning is understood. Privacy refers to the ability to control and manage the information that others can access about oneself. It involves setting boundaries regarding one's personal life and affairs, encompassing personal and family life, data protection, information about one's home, confidentiality and similar matters. External intrusion or influence should only occur with the individual's consent and in a manner that they accept. The right to respect for private life is limited to the extent that an individual brings their private life into contact with public life or connects it with other protected interests.¹² However, it can be challenging to expect minors below a certain age to be fully aware of the implications of their privacy. Parents are therefore expected to safeguard their child's privacy and promote the child's best interests.

In the physical world, the boundaries between private and public life are typically under the control of minors and their parents. Information exchange usually occurs through direct conversation or within a limited circle of individuals. The Internet has erased these boundaries, making communication less personal and more public.¹³ The omnipresence of social media, the Internet, and mobile communication in daily life has transformed both the social and legal landscape. This revolution brings many advantages that have made Internet adoption widespread, but it also has its drawbacks. From a legal perspective, the most endangered right is the right to privacy. This is particularly concerning in relation to children's rights, especially during adolescence, as privacy is crucial for children during this developmental stage.

Children are present in the digital world as much as adults, yet their presence is not proportional to their awareness of the potential risks. Children are exposed to online risks mainly in relation to their personal data, which are collected in various ways through different channels of communication on the Internet. The collection of personal data constitutes a violation of the right to privacy when it occurs without the individual's consent.¹⁴ However, an even greater danger lies in the purpose for which the collected data are used. In *Malone v. The United Kingdom* (1984), long before the digital era, the ECtHR observed that processed data, owing to advancements in computer technology, could be analysed in increasingly shorter timeframes, enabling the creation of a complete picture of a citizen's lifestyle.¹⁵ To understand the seriousness of such treatment of data, it is important to note that the Internet was not global at that time.

12 Dimitrijević, Paunović and Đerić 1997, p. 286. Regarding case law of European Court of Justice, see: *Couderc and Hachette Filipacchi Associés v. France* [GC], Application No. 40454/07, 10 November 2015, para.83. The right to privacy includes the right to use photos of the individual, and therefore right to refuse publication (*Von Hannover v Germany* (No. 2) [GC], Application No. 40660/08 and 60641/08, Judgement of 7 February 2012, para.96, HUDOC database.

13 DeVries, 2003, pp. 291-293.

14 Collecting personal data and its processing and publishing to a degree normally expected arises concerns on the right to privacy. See: *M.N. and others v San Marino*, Application No. 28005/12, Judgement of 7 July 2015, paras. 52-53. HUDOC database.

15 *Malone v. The United Kingdom*, Application No. 8691/79, Judgement of 2 August 1984. HUDOC database.

Sharing personal data, such as photos, videos, locations and other private information, is very prevalent among the young population and even their parents (known as “sharenting”).¹⁶ This trend opens the door to numerous forms of misuse, including advertising and marketing.¹⁷ In applications designed for young users, mobile advertising heavily relies on manipulative and disruptive methods.¹⁸ Much more serious and harmful to children are the abuse of personal data, identity theft, impersonation, Internet-based scams, and, in particular, contact with malicious individuals aiming to sexually or otherwise exploit a child (known as Internet predators), which can lead to cyberbullying.

The fast and widespread exchange of personal data in the digital environment is not the only risky aspect of Internet use. Complicating the issue further is that the storage capacity of Internet servers allows data, once uploaded, to remain there indefinitely. As a result, modern legal approaches have extended the right to privacy to include the “right to be forgotten” (or the right to erasure). This right, a product of case law, serves as a response to the need to protect privacy in the digital age. In a pioneering case, *Google Spain v. AEPD, Mario Costeja González*,¹⁹ the European Court of Justice was faced with the question of whether a complainant has the right to prevent access to disputed documents via a search engine in order to protect personal data. Although the right to be forgotten has been affirmed by the European Court of Justice, its function is limited to removing a specific link from the search engine index that would otherwise appear in search results when using an Internet browser. This applies only when the name and surname of a specific person are used as search criteria.²⁰ In contrast, in a case with a similar background, the ECtHR stated that judicial authorities are not competent to order the removal of a press article considered defamatory if it has been kept in a newspaper’s Internet archives.²¹ Later, the right to erasure received a normative framework within the European Union under the General Data Protection Regulation (Art. 17).²²

Comparing traditional and digital childhood, the distinction between private and public is no longer clear-cut.²³ The Internet operates as a new public space with partial privacy, since its boundaries are dictated by privacy settings. Even though

16 Shudra, 2023, pp. 88–105; Takhshid, 2023, pp. 1440–1449.

17 Johnson, 2022, pp. 158–159.

18 Verdoodt, 2019, pp. 466–468.

19 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Judgement of the Court, 13 May 2014, C-131/12.

20 Midorović, 2019, p. 285.

21 *Wągrzynowski and Smolczewski v Poland*, Judgement of 20 October 2015, Application No. 25239/13, HUDOC database paras. 39–41. *Satakunnan Markkinapörssi Oy and Satamedia v Finland*, Judgement of 27 June 2017, Application No. 931/13. HUDOC database.

22 Regulation (EU) 2016/679 of the European Parliament and of the Council 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), *Official Journal of the European Union*, L119, 4 May 2016.

23 Thompson, 2011, p. 49.

privacy settings allow users to modify their privacy preferences, they have limited potential, as users are merely making choices within the available technical solutions. Moreover, these settings are often governed by self-regulation rules.

To conclude, the protection of privacy online involves employing a variety of strategies, such as understanding encryption systems, adjusting privacy settings on specific Internet platforms, interpreting numerous privacy policies, and navigating complex information technology systems. Therefore, it is important to discuss the new form of “digital literacy” necessary to secure at least a certain level of privacy on the Internet.²⁴

6.2. Right to Education

The CRC stipulates the right to education (Art. 28), encompassing both formal and informal dimensions. From a formal perspective, primary education is made compulsory and free for all. The development of secondary and higher education is encouraged and made available and accessible to every child, in accordance with the principle of non-discrimination. Informal education refers to the development of knowledge outside institutional settings, as well as lifelong learning.

The right of parents to influence the education of their children – that is, to provide education and teaching in accordance with their religious and philosophical beliefs – is guaranteed in the second sentence of Art. 2 of Protocol No. 1 to the ECHR. In drafting this provision, great importance was placed on family life during education, while the role of the state was made secondary.²⁵ The ECtHR has interpreted this provision in light of respecting private and family life, freedom of thought, conscience and religion, as well as freedom of expression under the ECHR.²⁶ The Court reached this conclusion after examining whether the responsible state ensured that the knowledge included in the curriculum for the disputed subject was transmitted in an objective, critical and pluralistic manner, or whether indoctrination was sought, disregarding the religious and philosophical beliefs of the applicant’s parents. In a case related to parents’ objection to compulsory sex education in public schools, the Court did not find a violation of parental rights in children’s education. The Court examined the nature of the measure and pointed out that it was not aimed at promoting particular sexual behaviours. Thus, the subjective views of parents are not relevant in the decision-making process; rather, objective criteria must be applied.²⁷ Regarding the challenges of the digital age, in 2009, the ECtHR pointed out that parents cannot deny a child’s

24 Moll and Pieschl, 2016, p. 239.

25 Unlike this provision, the CRC provides for the right of the child than of the parents, as stipulated in the cited provision of ECHR; Hale, 2006, 351.

26 *Folgero and Others v. Norway* [GC], Judgment of June 29, 2007, Application no. 15472/02, HUDOC database, para. 84.

27 *Kjeldsen, Busk Madsen And Pedersen v. Denmark*, Judgment of December 7, 1976, Application No. 5095/71; 5920/72; 5926/72, HUDOC database; *A.R. and L.R. v. Switzerland* (No. 22338/15) [Online]. Available at: https://www.echr.coe.int/documents/d/echr/FS_Childrens_ENG (Accessed 15 January 2024).

right to education based on their personal beliefs. Specifically, the Court dismissed as inadmissible an application that concerned the refusal of permission for parents to educate their children at home in accordance with their religious beliefs.²⁸

Digital technology has undoubtedly changed the environment for education in both senses. The Committee on the Rights of the Child states:

‘... the digital environment can enable and enhance children’s access to high-quality, inclusive education, including reliable resources for formal, non-formal, informal, peer-to-peer, and self-directed learning. The use of digital technologies can also strengthen engagement between teachers and students, as well as among learners. Children have highlighted the importance of digital technologies in improving their access to education and in supporting their learning and participation in extracurricular activities.’²⁹

Digital technology enables children to learn in both formal and informal contexts. Acquiring various competencies necessary for successful functioning in the digital age includes digital, linguistic, mathematical, and scientific literacy; problem-solving skills; critical thinking; teamwork; and learning foreign languages. Digital technology has enabled children to have free access to quality educational resources, programmes, applications and platforms for various purposes. They can virtually visit museums and libraries. Despite the advantages of accessible digital knowledge, the enforcement of the right to education in terms of technology is complicated. Access to digital devices and the Internet represents a necessary, but not sufficient, condition for their safe and constructive use. Thus, the first challenge is that digital education requires digitally skilled teachers and parents, who should oversee children as they go through the educational process. Modern education must provide children with the skills for the safe and constructive use of digital technology in various life situations. In professional literature, these skills are often referred to as digital literacy and digital competence.³⁰

The concept of literacy in the digital environment is more complex than its traditional meaning. Traditionally, literacy refers to the skills of writing, reading and arithmetic. In the modern, digital world, it encompasses a set of knowledge, skills and attitudes necessary for using digital technology to perform various tasks, solve problems, communicate, manage information, collaborate, create and share content, and construct knowledge in an efficient, effective, critical, creative, autonomous, flexible, ethical and reflective manner. These skills are essential not only for work and leisure but also for participation in society, learning and socialising. Additionally, the

28 *Konrad v. Germany*, Decision of September 11, 2009, Application No. 35504/03, HUDOC database.

29 General comment No. 25 (2021) on children’s rights in relation to the digital environment, 17. See: Djeflal, 2022, pp. 1–9.

30 European Commission, Directorate-General for Education, Youth, Sport and Culture, 2019.

process of acquiring digital literacy should involve adults, particularly parents and teachers, alongside children.

Creating an appropriate climate for learning in the digital world can significantly impact the development of qualified and competitive citizens in the future. However, this advantage is not universal. Not all children can afford computer technology, which is a prerequisite for enjoying the benefits of digitalisation. This disparity could deepen inequalities among students³¹ – one of the reasons for the increasing demand to establish the universal right to access the Internet.³²

6.3. Right to Information

According to Art. 17 of the CRC, recognising the important role played by the mass media,³³ states shall ensure that children have access to information and materials from a diversity of national and international sources, especially those aimed at promoting their social, spiritual and moral well-being, as well as their physical and mental health. States are encouraged to exchange and disseminate information and materials of social and cultural benefit to children, produce and distribute children's books, and cooperate internationally in the production and dissemination of such materials. The mass media are encouraged to consider the linguistic needs of children belonging to minority or indigenous groups. Lastly, states should develop appropriate guidelines for protecting children from information and materials that may be harmful to their well-being.

The right to information forms part of the cognitive and social development of the child, as information plays a significant role in shaping the child's identity and personality, thus influencing their participation in society. As such, the right to information is a precondition for the full exercise of other human rights, such as the right to education, freedom of expression, and freedom of thought. Moreover, the right to information is an essential component of communication, which lies at the core of a child's life and development.

Compared with other rights, the right to information is less visible as an individual entitlement and more visible as a public concern. Typically, its realisation depends on a broad range of state regulations. From a positive perspective, in terms of encouraging the provision of information, states guarantee the right by regulating public institutions such as libraries, media outlets or materials used in the educational process. When regulating these tasks, the selection of information available to children should be carefully managed to protect their dignity and safety, while also preserving cultural, social and other values.

31 Gustin, 2022, p. 469. Reminding COVID-19 pandemic, computer infrastructure and information technology contributed a lot in overcoming the extended period of closure, especially regarding the education tasks.

32 In his Report, António Guterres suggests universal access to the Internet by 2030 as a basic human right. See: *Our Common Agenda – Report of the Secretary-General*, United Nations, 2021, p. 4.

33 Hammarberg, 1997, p. 249 and p. 253.

Considering the nature of the digital world and digital communication, particularly the Internet, the right to information is, in a certain sense, controversial. The global nature of the Internet allows children to access more information than ever before. Information flows from a wide range of communication channels, offered by diverse individuals and institutions from different countries, cultures and religions. The sheer volume of information is crucial for the exercise of the right to information, as well as for acquiring knowledge and personal development.

However, children who can access the Internet and various websites without sufficient oversight of their eligibility to do so are still in the process of developing the skills needed to evaluate and process the information they receive. Therefore, enforcing the right to information without proper safeguards could harm other rights of children, as well as the rights of others. For this reason, the right to information, in line with the CRC, must also limit access to certain information (though not explicitly stated in the CRC), in accordance with national laws.

The Internet complicates the right to information. The exchange of information is not entirely under the control of national authorities. Even when national regulations apply, they may not cover all cases. Social networks, which play a major role in children's communication, are not typically classified as media and thus fall outside the scope of national laws governing public information. Instead, they are often self-regulated.

Another contentious issue is who controls the information that children access on the Internet. The dominant sources of information are usually adults, which can distort the framework of a child's world. As a result, the full potential of the right to information cannot be realised without the active involvement of children in the exchange of relevant information. This, in turn, brings us to the right to expression. According to Art. 13 of the CRC, the freedom to seek, receive and impart information is a core part of the right to freedom of expression.

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

The crucial outcome of the CRC is the recognition that a child possesses individuality, evident both within the family and in the broader social environment. This recognition marks a significant achievement in advancing the child's position in society. However, the child is not an entirely independent person. The extent of a child's autonomy depends on their age and maturity. This is a natural consequence of the fact that children require the support and guidance of their parents and society until they gain independence. While a child has a unique individuality that should be expressed, they still require support, assistance and understanding throughout their development and upbringing. The ability of the child to make decisions is especially important here. Therefore, the CRC guarantees freedom of expression as a fundamental human right.

According to Art. 12, a child who is capable of forming their own views has the right to express those views freely on all matters affecting them, in accordance with their age and maturity. Art. 13 of the CRC stipulates that every child has the right to

freedom of expression. This includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, whether orally, in writing, in print, in the form of art or through any other media of the child's choice. This right may be subject to certain restrictions in accordance with national laws, specifically to respect the rights of others and maintain public order, as explicitly prescribed in Art. 10 of the ECHR.³⁴ The true power of this right originates from the integrative aspect of the relevant provision, which guarantees the child's right to be heard. Specifically, the CRC provides children with the opportunity to express their views in any judicial or administrative proceedings affecting them, either directly or through a representative or an appropriate body.³⁵

When fully observed, the right to participation is one of the core rights in the CRC and has evolved into a fundamental principle of modern children's rights law. It is, at its essence, a right of participation. Although this right is explicitly mentioned in relation to procedures affecting the child, it is not limited to these matters alone. The full potential of children's participation extends to decisions about activities in their free time, such as choosing sports, arts or other hobbies. However, the child's right to participate also implies a responsibility for adults to create opportunities to realise that right. Participation does not mean placing the child in opposition to the views and values of adults; rather, it involves creating a space where, together, children and adults can make decisions that impact them both.

The digital age and Internet communication pose significant challenges to the right to participation in all its aspects. Children today live in an age of vast information, readily accessible on the Internet, yet they often lack the skills to assess the source and authenticity of that information. Adults, too, are not always equipped to help, as they may not be fully competent in evaluating digital content. As a result, the goal of fostering responsible, self-confident and socially reliable individuals through children's participation is increasingly called into question. Even the very act of decision-making is subject to the digital revolution. One such challenge is the rise of artificial intelligence, which continues to grow in influence. Today, children frequently use machine learning tools to solve even simple daily tasks. This digital environment not only threatens children's rights but also raises concerns about the future of humanity. Therefore, children's rights are more crucial than ever as a matter of public interest, demanding decisive action from all relevant actors, particularly authorities, to strike a balance between traditional values, technological advancements and the social good.

34 Analysis on the freedom of expression in certain Central European countries is published by Ferenc Mádl Institute for Comparative Law; Wielec, 2021.

35 Sawyer, 1999, pp. 155–157.

7. Role of Parents in the Protection of Children's Rights

Before the advent of the digital revolution, the issue of the best interests of the child and the role of parents in implementing the child's rights primarily focused on decisions concerning the child's health, education, guardianship in cases of parental separation, and other matters related to family dynamics in the physical world. Parents have the autonomy to raise their children according to their own values and beliefs. Caring for the child is not only a duty but also a right of the parents. The state only plays a corrective role if one or both parents lack the capacity to act in the best interests of the child. Parental autonomy is limited by state authority where necessary, and by the child's autonomy when the child is capable of expressing their opinion.³⁶ However, the parent-child relationship has gradually shifted towards the concept of trusteeship.³⁷

The Internet has brought parental authority into question. Even well-intentioned parents often find themselves caught in the trap of global communication. Rather than protecting their child's rights, parents frequently and unknowingly compromise these rights.³⁸ The 21st century is the era of increased publicity, driven largely by social media and social networks.³⁹ Parental rights are often exercised through the freedom to share moments of daily family life. In some cases, this phenomenon, known as "sharenting", becomes excessive, where parents, particularly mothers, publicly document every stage of their child's life – from pregnancy to the child's 18th birthday and beyond. Such practices create challenges in recognising the child's rights as individual rights, especially since children's rights are closely tied to the rights of family members, which can sometimes conflict.⁴⁰ Parents often overlook the best interests of the child – not owing to intentional neglect but owing to their struggle to keep pace with the rapid technological revolution. As a result, they are not adequately prepared to fulfil their responsibility in safeguarding their child's well-being in the digital age.⁴¹ Now more than ever, parents – as the primary guardians of their children – need the support of state authorities.⁴² This support should include informal education for parents, counselling and involvement in their children's activities. In extreme cases, state intervention may include measures against parents whose behaviour could harm the child's well-being.

36 Kovaček Stanić, 2022, p. 78.

37 Sorensen, 2016, p. 157.

38 Sorensen, 2016, p. 156.

39 Joyce, 2013, pp. 233–234.

40 Sorensen, 2016, p. 166.

41 Haubenreich, 2009, p. 242.

42 Sorensen, 2016, p. 174.

Bibliography

- Choudhuri, A. (2019) 'Conceptualizing Children's Rights in Digital Spaces: Emerging Issues and Challenges', *Socio-Legal Review*, 15(2), pp. 151–179; <https://doi.org/10.55496/NTPF6562>.
- Council of Europe (2018) *Guidelines to respect, protect and fulfil the rights of the child in the digital environment – Recommendation CM/Rec(2018)7 of the Committee of Ministers, Building a Europe for and with Children*. Strasbourg: Council of Europe p. 16 [Online]. Available at: <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a> (Accessed: 10 January 2024).
- DeVries, W.T. (2003) 'Protecting Privacy in the Digital Age', *Berkeley Technology Law Journal*, 18(1), pp. 283–312; <https://doi.org/10.15779/Z38T97M>.
- Dimitrijević, V., Paunović, M., Đerić, V. (1998) *Ljudska prava - udžbenik*. Belgrad: Beogradski centar za ljudska prava.
- Djeffal, C. (2022) 'Children's rights by design and Internet governance: Revisiting general comment No. 25 (2021) on children's rights in relation to the digital environment', *Laws*, 11(6), pp. 1–9.
- European Commission, Directorate-General for Education, Youth, Sport and Culture (2019) *Key competences for lifelong learning*. Luxembourg: Publications Office [Online]. Available at: <https://data.europa.eu/doi/10.2766/569540> (Accessed: 20 December 2023).
- Franco, L. Almog, S. (2019) 'Precarious Childhood: Law and Its (Ir)Relevance in the Digital Lives of Children', *Penn State Journal of Law and International Affairs*, 7(1), pp. 53–87.
- Grover, S. (2004) 'On Recognizing Children's Universal Rights: What Needs to Change in the Convention on the Rights of the Child', *International Journal of Children's Rights*, 12(3), pp. 259–272; <https://doi.org/10.1163/1571818042885976>.
- Gustin, M. (2022) 'Challenges of Protecting Children's Rights in the Digital Environment', *EU and Comparative Law Issues and Challenges*, 2022/6, pp. 453–488; <https://doi.org/10.25234/eclic/22439>.
- Hale, B. (2006) 'Understanding children's rights: theory and practice', *Family Court Review*, 44(3), pp. 350–360; <https://doi.org/10.1111/j.1744-1617.2006.00093.x>.
- Hammarberg, T. (1997) 'Children, the UN convention and the media', *International Journal of Children's Rights*, 5(2), pp. 243–262; <https://doi.org/10.1163/15718189720493636>.
- Haubenreich, S.N.S. (2009) 'Parental Rights in Myspace: Reconceptualizing the State's Parens Patriae Role in the Digital Age', *Hastings Communications and Entertainment Law Journal*, 31(2), pp. 223–256; <https://doi.org/10.2139/ssrn.1217872>.
- Johnson, H. (2022) 'Marketing Research and Children's Consumer Privacy Rights: Battle in the Digital Age', *Barry Law Child and Family Law Journal*, 2022/10, pp. 154–176.

- Joyce, D. (2013) 'Media Witness: Human Rights in an Age of Digital Media', *Intercultural Human Rights Law Review*, 2013/8, pp. 231–280.
- Kovaček Stanić, G. (2022) 'Parental Autonomy v. Child Autonomy v. State Authority Powers', *Law, Identity and Values*, 2(2), 65–82; <https://doi.org/10.55073/2022.2.65-82>.
- Midorović, S. (2019) 'Pravno na brisaje podataka o ličnosti dostupnih na Internetu', *Zbornik radova Pravnog fakulteta u Nišu*, 58(84), pp. 281–306; <https://doi.org/10.5937/zrpfno-22953>.
- Moll, R., Pieschl, S. (2016) 'Expecting Collective Privacy: A New Perspective on Trust in Online Communication' in Blöbaum, B. (ed.) *Trust and Communication in a Digitized World: Models and concepts of trust research*. Cham: Springer, pp. 239–251; https://doi.org/10.1007/978-3-319-28059-2_14.
- Papandrea, M.R. (2008) 'Student Speech Rights in the Digital Age', *Florida Law Review*, 60(5), pp. 1027–1102.
- Savić, I. (2019) '30 years after the adoption of the Convention on the rights of the child' in Pavlović, Z. (ed.) *Yearbook – Human rights protection – protection of the rights of the child*. Novi Sad: Provincial Protector of Citizens, pp. 301–317.
- Sawyer, C. (1999) 'One Step forward, Two Steps Back – The European Convention on the Exercise of Children's Rights', *Child and Family Law Quarterly*, 11(2), pp. 151–166.
- Shudra, T. (2023) 'Children's personal data protection in digital environment with different expectations between parents and children', *Journal of Personal Data Protection Law*, 1(1), pp. 88–105.
- Skoler, D.L. (1993) 'The U.N. Children's Convention', *Family Advocate*, 15(4), pp. 38–41.
- Sorensen, S. (2016) 'Protecting children's right to privacy in the digital age: parents as trustees of children's rights', *Children's Legal Rights Journal*, 36(3), pp. 156–176.
- Thompson, J.B. (2011) 'Shifting Boundaries of Public and Private Life', *Theory, Culture and Society*, 28(4), pp. 49–70; <https://doi.org/10.1177/0263276411408446>.
- Verdoodt, V. (2019) 'The Role of Children's Rights in Regulating Digital Advertising', *International Journal of Children's Rights*, 27(3), pp. 455–481; <https://doi.org/10.1163/15718182-02703002>.
- Wielec, M. (ed.) (2021) *The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism – Analysis on Certain Central European Countries*. Budapest–Miskolc: Ferenc Mádl Institute of Comparative Law, Central European Academic Publishing; <https://doi.org/10.54237/profnet.2021.mwsm>.
- Worldometers (n.d.) 'Population' [Online]. Available at: <https://www.worldometers.info/> (Accessed: 20 November 2023).

European Law

András KOLTAY

ABSTRACT

The Internet and digitalization make easier to find information, learn, work, or even entertain, however, it can also give platform to harmful contents and bad practices. The latter two takes many forms, from strong language and unethical marketing strategies to child pornography and bullying. The European Union tries to protect its citizens, especially youth, from cybercrime, and prepare them for the challenges evolving in the online world. This chapter gathers the measures, soft law means and regulations the European Union created to prevent children becoming online victims, and shows not only the related international conventions but the relevant legal cases as well, giving a more complex and comprehensible account of the risks and dangers everybody, especially minors, have to face on the Internet.

KEYWORDS

protection of minors, internet regulation, cyberbullying, child pornography, harmful content

1. Introduction

In addition to the many benefits of digitalisation, there are also many security risks, which can pose threats to children. Therefore, defending against them is of paramount importance in the digital space, which several international and European Union (EU) documents aim to ensure. These documents can be divided into three categories: soft law, legislation, and court judgments:

- soft law material includes documents adopted by international organisations and the EU that are not legally binding (e.g. strategies, action plans, and guidelines);
- legislation includes international conventions that have been transposed into national law by the States Parties, as well as EU acts;
- court judgments are final decisions of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

András KOLTAY (2025) 'European Law' in Halász, Cs. (ed.) (2025) *Children in Digital Age*. Miskolc-Budapest: Central European Academic Publishing, pp. 67–86. https://doi.org/10.71009/2025.csh.cida_4.

Most soft law documents and legislation explicitly provide for children’s rights in the context of digitalisation. Some documents are not about digitalisation, but the nature of the protection they contain can also apply to the protection of children in the digital space. For example, the United Nations (UN) Convention on the Rights of the Child, which predates the mass use of the Internet. Most of the EU documents are soft law, but some legal acts also contain provisions that regulate children’s rights in the context of the digital space. At the international level, the UN Convention on the Rights of the Child and the Council of Europe’s Lanzarote Convention on the protection of children against sexual exploitation are the most comprehensive relevant documents, while at the EU level, the EU Strategy on the Rights of the Child should be highlighted. As regards the relevant case law at both international and EU levels, most of the judgments are only partially relevant to children’s rights in the context of digitalisation.

2. International Rules and Case Law

2.1. *Soft Law Documents*

Under the auspices of the UN, there are several documents that are not legally binding, but which refer to or can be linked to the need to protect children in the digital space. The following are brief summaries of relevant guidelines, roadmaps, and reports produced by the United Nations Educational, Scientific and Cultural Organization (UNESCO), the United Nations Children’s Fund (UNICEF), and the United Nations Human Rights Council.

The UNESCO roadmap Education for Sustainable Development 2020–2030 (ESD)¹ refers to the benefits and challenges of digitalisation. As examples of the former, it cites the expected improvement in quality of life; and of the latter, the following relevant security risks: artificial intelligence (AI) applications can strongly influence human behaviour in consumption or social interactions, and the unequal sharing of the benefits of technological progress can increase the gap between the “haves” and the “have-nots”. To meet these challenges, the ESD must also prepare future generations. In comparison, the Guidance for generative AI in education and research (2023)² aims to support countries in implementing immediate actions, designing long-term policies, and building human capacity for a human-centred vision of AI. The Guidance provides concrete recommendations for policymakers and educational institutions on how to design the use of generative AI tools to truly benefit students, teachers, and researchers. Both UNESCO’s World Youth Skills Day 2023: Empowering youth for a sustainable future³ report and the Transforming Technical and Vocational

1 UNESCO, 2020.

2 Fengcun and Wayne, 2023.

3 UNESCO, 2023.

Education and Training for successful and just transitions (2022–2029)⁴ strategy have similar objectives. The former is aimed at enabling young people to adapt effectively to changing labour market conditions because of technological progress. The document includes a specific chapter on the need to strengthen digital and AI-related skills in education. The latter, pointing to the changes in the labour market brought about by digitalisation, similarly states that young people’s training must adapt to these new conditions. The aim is to strengthen skills in education that will enable young people to be competitive in the labour market.

Among UNICEF’s documents, the Education Strategy (2019–2030),⁵ which, under the heading “Goals”, mentions the development of children’s digital skills and knowledge, including the ability to search and manage information, communicate, collaborate, create and share content digitally, and solve problems safely, critically, and ethically, should be highlighted. Worthy of mention are the Guidelines for journalists reporting on children,⁶ which aim to ensure that children’s rights and safety are also guaranteed when reporting on children or covering children’s issues. The rules are not just limited to the digital space, but the flow of information revolutionised by digitalisation means that content about children can also reach huge audiences. As such, with the development of digitalisation, the guide is particularly relevant to the protection of children in the digital space.

Finally, of the international sources that are not legally binding, the Annual reports of the UN Human Rights Council should be highlighted.⁷ Every year, the Council issues such documents, which also place a strong emphasis on child protection and are available on its website going back to 2006. On the protection of children in the digital space, child pornography appears in all reports, whereas cyberbullying has been a common theme in reports since 2014.

2.2. International Conventions Enacted in Law

In addition to soft law instruments, several legally binding international conventions have been concluded in recent decades that either explicitly aim to protect children’s rights or contain child protection provisions. The following are the provisions that are intended to provide protection in the digital space or may be relevant for this type of protection.

The UN Convention on the Rights of the Child (1991)⁸ does not contain an explicit provision on the protection of children in the digital space, one obvious reason being that it was adopted before the widespread use of the Internet. However, some of its articles are clearly applicable to this protection. According to Article 16, no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, or to unlawful attacks on their honour and reputation.

4 UNESCO, 2022.

5 UNICEF, 2019.

6 UNICEF, n.d.

7 United Nations, n.d.

8 United Nations General Assembly, 1989.

This provision also provides protection in cases where the child is subjected to such abuse in the online space. Article 17 states, in relation to the right to access information from the mass media, that States Parties should encourage the development of appropriate guidelines for the protection of the child from information and material injurious to their well-being. Article 18 emphasises that both parents have common responsibilities for the upbringing and development of the child. The provision can also be interpreted as a responsibility for the child's presence in the digital space. Article 34, which aims to protect the child from all forms of sexual exploitation and pornography, can also apply to the digital space.

Like the Convention, the Optional Protocol to the Convention on the Rights of the Child (2009)⁹ does not contain a specific provision aimed at protection in the digital space, but in its Article 1, it requires States Parties to prohibit, *inter alia*, child pornography, and in Article 3, it obliges States Parties to ensure that child pornography is fully covered under their criminal law. In its Preamble, the Protocol warns of the growing availability of child pornography on the Internet and other evolving technologies. It also refers to recalling the International Conference on Combating Child Pornography on the Internet (Vienna, 1999) and its conclusion calling for the worldwide criminalisation of the production, distribution, exportation, transmission, importation, intentional possession, and advertising of child pornography.

Several relevant provisions are contained in the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse ('Lanzarote Convention', 2015),¹⁰ which aims, in general, to prevent and combat sexual exploitation and sexual abuse of children, to promote national and international cooperation to this end, and to protect the victims' rights. The document contains provisions specifically aimed at protecting against sexual exploitation and abuse in the digital space.

Article 6 obliges States Parties to ensure that children, during their education, receive adequate information on the risks of sexual exploitation and sexual abuse, as well as on the means of protecting themselves. Special attention must be paid to situations of risk involving the use of new information and communication technologies (ICT). Article 9 also requires the ICT sector to participate in drawing up and implementing policies to prevent sexual exploitation and sexual abuse of children. The same article states that each Party shall encourage the media to provide appropriate information concerning all aspects of sexual exploitation and sexual abuse of children. Article 20 commits Parties to take the necessary legislative or other measures to ensure that the intentional offences of child pornography, when committed without right, are criminalised. However, under the Convention, Parties may reserve the right not to consider as the production of child pornography, or knowingly accessing child pornography through ICT technologies, the production and possession of pornographic material consisting exclusively of simulated representations or

9 United Nations General Assembly, 2000.

10 Council of Europe, 2007.

realistic images of a non-existent child, involving children who have reached the age below which it is prohibited to engage in sexual activities with a child, where these images are produced and possessed by them with their consent and solely for their own private use.

Pursuant to Article 30, the Parties shall take the necessary measures to enable the investigative services to identify the victims of the offences established in accordance with Article 20, by analysing child pornography material, such as photographs and audiovisual recordings. Article 21 obliges Parties to take the necessary measures to ensure that intentional pornographic conduct involving children is criminalised. Article 22 provides for the criminalisation of the corruption of children. Accordingly, the Parties shall take the necessary legislative or other measures to criminalise intentionally causing, for sexual purposes, a child who has not reached the age above which they may be allowed to engage in sexual activities, to witness sexual abuse or sexual activities, even without having to participate. Article 23 requires Parties to criminalise the solicitation of children for sexual purposes. This is when an adult makes an intentional proposal, through information and communication technologies, to meet a child who has not reached the age above which they may be allowed to engage in sexual activities, for the purpose of engaging in sexual activity or producing child pornography. It is a condition that the proposal has been followed by material acts leading to such a meeting.

The implementation of the Lanzarote Convention is monitored by the Lanzarote Committee of the Council of Europe. On 17 June 2015, the Committee adopted an opinion on Article 23 of the Convention, inviting States Parties to consider the possibility of criminalising sexual abuse in cases where it is not the result of a face-to-face encounter but takes place online.¹¹

Another important source of international law of the Council of Europe is the Budapest Convention on Cybercrime (2001),¹² Article 9 of which obliges Contracting Parties to take all legislative and other measures to establish, as a criminal offence, the production, offering, making available, transmitting, distributing, procuring, or possessing child pornography through a computer system, when committed intentionally and without right.

Although facilitating the cross-border transmission of television programmes is the fundamental objective of the European Convention on Transfrontier Television (1989),¹³ with the advent of digital television, certain provisions of this document may also apply to the protection of children in the digital space. Under Article 7, all items of programme services, as concerns their presentation and content, shall respect the dignity of the human being and the fundamental rights of others. They shall not be indecent, contain pornography, or give undue prominence to violence or be likely to incite racial hatred. Any parts of programme services that are likely to impair

11 European Union Agency for Fundamental Rights, Council of Europe, 2015, p. 141.

12 Council of Europe, 2001.

13 Council of Europe, 1989.

the physical, mental, or moral development of children and adolescents may not be scheduled for when, because of the time of transmission and reception, they are likely to watch them. In relation to advertising, Article 11(3) states that advertising and tele-shopping addressed to or using children must avoid anything likely to harm their interests and shall have regard to their special susceptibilities.

2.3. Case Law of the European Court of Human Rights

Of relevance to the protection of children's rights in the digital space are Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which guarantees respect for private and family life, and Article 10, which guarantees freedom of expression. The provisions of the Convention may be enforced through proceedings initiated before the ECtHR. Hence, if a private individual considers that a State Party has violated a Convention right, they may, after exhausting their remedies at the national level, apply to the ECtHR, the judgment of which the State is obliged to implement.

Under Article 8, everyone has the right to respect for their private and family life, their home, and their correspondence. However, the ECHR also specifies the cases in which the State may interfere with the exercise of this right. These include the prevention of crime and the protection of public health, morals, and the rights and freedoms of others. Article 10 states that everyone has the right to freedom of expression, adding that States may require the licensing of broadcasting, television, or cinema enterprises. In this case, too, the text lays down specific cases of restriction of the right, particularly the prevention of crime, the protection of health, morals, the reputation or rights of others, and the prevention of the disclosure of confidential information.

From the above, it can be seen that the ECHR requires, above all, a kind of abstention from States in the exercise of these rights. However, if a listed interest justifies it, the State must take an active approach. Therefore, where a child user in the digital space is threatened by a crime or a risk to their health or moral well-being, or where it is necessary to protect their reputation or rights, the State is expected to act to take measures to protect the child. The cases listed below are closely related to the issue of protecting children in the digital space.

In the *K.U. v. Finland*¹⁴ case, an advertisement was published on behalf of a 12-year-old boy on an online dating site without his knowledge, which included his age, telephone number, and a detailed description of his physical characteristics, along with a link to his website, which included his picture. It also suggested that the child was seeking an intimate relationship with a boy of his age or older. The legislation in force did not allow the identity of the advertiser to be obtained from the Internet service provider (ISP). In the case, the ECtHR ruled that the boy's physical and moral well-being was endangered, as he was exposed as a target for paedophiliac

14 *K.U. v. Finland*, No. 2872/02.

approaches. This violated his right to respect for private and family life, as enshrined in Article 8 of the ECHR.¹⁵

In *Rothe v. Austria*,¹⁶ the applicant, Wolfgang Rothe, was the head of a Catholic seminary and was the subject of a newspaper article in 2004 alleging that he had a homosexual relationship with one of his students. The police had searched the seminary on suspicion of someone having downloaded child pornography from the Internet. Rothe brought proceedings against the newspaper for defamation and invasion of privacy, but the national court rejected his case. Rothe appealed to the ECtHR, which argued that the public had an interest in knowing about the situation at the seminary regarding the downloading of child pornography. The panel compared the applicant's right to respect for private life under Article 8 of the Convention with the right to freedom of expression under Article 10 and decided that Article 8 had not been violated.¹⁷

The main case of *Benedik v. Slovenia*¹⁸ dates to 2006, when the Swiss police informed the Slovenian law enforcement authorities of the identification of a dynamic internet protocol(IP) address linked to sharing material containing the sexual abuse of children. The Slovenian police ordered the Slovenian ISP to disclose the user data linked to the IP address without a preliminary court order. In response to the request, the ISP provided the police with the name and address of the subscriber to the Internet service associated with the IP address, but the case was charged against the subscriber's son. The applicant argued that he was not aware of the content of the online material in question but was nevertheless convicted of manufacturing, possessing, and distributing child sexual abuse material. The applicant exhausted all remedies available in Slovenia, arguing that evidence of his identity was acquired unlawfully because the authorities did not have a prior court order to obtain subscriber information related to the IP address. The case was referred to the ECtHR, which upheld the applicant's claim that his right to respect for private and family life under Article 8 of the Convention had been violated.¹⁹

The case of *Kharitonov v. Russia*²⁰ also relates to the legal assessment of online activity. The applicant was a person living in Moscow, who owned a website called Electronic Publishing News, founded in 2008. The website was hosted by a U.S. web hosting service provider together with other websites sharing the same IP address. In 2012, the Russian telecommunications regulator ordered all websites associated with the IP address to be blocked because of the availability of content promoting drugs, which is dangerous for children, on one website, rastaman.tales.ru. The applicant initiated legal proceedings against the Authority's decision, claiming that it also rendered inaccessible websites associated with the same IP address, but not

15 European Union Agency for Fundamental Rights, Council of Europe, 2015, p. 72.

16 *Rothe v. Austria*, No. 6490/07.

17 Human Rights Guide, 2012.

18 *Benedik v. Slovenia*, No. 62357/14.

19 Chatzinikolaou, 2018.

20 *Vladimir Kharitonov v. Russia*, No. 10795/14.

publishing infringing content. The case was referred to the ECtHR, which found that the applicant's right to freedom of expression under Article 10 of the Convention, and to an effective remedy under Article 13, had been violated.²¹

In *X and Others v. Bulgaria*,²² an Italian couple adopted three children from an orphanage in Bulgaria in 2012. The couple subjected the children to a psychological assessment, which led to the conclusion that they had allegedly been subjected to constant sexual abuse in the orphanage, of which pornographic recordings had been made. The Bulgarian authorities opened an investigation into the case, which was later closed as there was no evidence of a crime. The case was eventually referred to the ECtHR on the grounds that the Bulgarian authorities had breached the Convention by failing to fulfil their obligations to protect the children and to investigate. The Court ruled that the authorities' action was insufficient to ensure the purpose of Article 3, which prohibits torture.²³

The case of *Macatė v. Lithuania*²⁴ is relevant in the context of the legal assessment of the online publication of books. The main case reports that, in Lithuania, a children's fairy-tale book containing stories about same-sex marriage was published in 2013 by the Lithuanian University of Educational Sciences and made available online several times without restrictions. The book was widely disliked and, following a critical letter from eight members of Parliament, the university rector ordered the suspension of its distribution. The case was referred to the ECtHR, which found that the suspension violated the author's right to freedom of expression under Article 10 of the Convention.²⁵

3. European Union Regulations and Case Law

3.1. Soft Law Documents

The EU places a strong emphasis on both child protection and digital security, as reflected in the many strategic documents on these issues. The following list contains relevant, non-normative strategies, action plans, and recommendations that call for greater protection of children in the digital space.

One of the most important general child protection documents is the EU Strategy on the Rights of the Child (2021).²⁶ The Strategy states that digital technologies offer children a wide range of opportunities for learning, entertainment, and future employment. However, access to the Internet remains a challenge for many children in the EU. The Strategy also draws attention to the impact of AI on children's rights and child safety. It promotes the development of accessible ICT technologies for children

21 Ibid.

22 *X and Others v. Bulgaria*, No. 22457/16.

23 EU Law Live, 2023.

24 *Macatė v. Lithuania*, No. 61435/19.

25 Milkaitė, 2023.

26 European Commission, 2021a.

with disabilities. It will also step up the fight against all forms of online sexual abuse of children, for example, by proposing legislation to require online service providers to detect and report child sexual abuse material. The document also sets out concrete actions for Member States to improve access to digital tools, the Internet, digital literacy, and media literacy. The Strategy also calls for ICT companies to take measures to ensure children's rights, to prevent Internet addiction and harmful and illegal content on the Internet, to detect such content, and to use effective age verification tools.

The communication on Europe's Digital Decade sets ambitious connectivity targets for European households and aims to ensure child protection. It highlights that children can be victims, witnesses, and perpetrators of violence online. The communication makes it clear that children's mental health problems can be linked to the persistent use of digital devices. Its goals also include the digital and information society: an EU where children can safely use and benefit from the digital environment.

The 2030 Digital Compass²⁷ sets out the European way for the digital decade, which includes a focus on child protection as well. The document points out that broad-based digital skills must also build a society in which children learn how to understand and navigate through the myriad of information to which they are exposed online. In addition, a human-centred, secure, and open digital environment must also enable children's rights to be enforced. It is important to develop a comprehensive set of digital principles, such as the protection and empowerment of children in the online space.

The new strategy for a better internet for kids (BIK+)²⁸ aims to ensure that children are protected, respected, and empowered online in the new digital decade. The document also sets out specific measures for Member States and the industry. Examples include Member States supporting effective age verification methods, and digital education for adults by children; industry working with trusted flaggers to assess and remove illegal content quickly and developing products and services that promote children's right to express themselves, and that facilitate their participation in public life.

The European Union's Strategy for a more effective fight against child sexual abuse²⁹ aims to provide a comprehensive response to the growing threat of child sexual abuse online and offline. This document constitutes the EU's reference framework for action to combat child sexual abuse for the period 2020–2025. In the Strategy, the Commission has expressed its intention to cooperate with businesses, civil society organisations, higher education institutions, professionals, researchers, law enforcement, other public authorities, and stakeholders to ensure the implementation of the eight initiatives outlined in the Strategy (for example, strengthening industry efforts to ensure the protection of children in their products).

27 European Commission, 2021b.

28 European Commission, 2022.

29 European Commission, 2020a.

In its Resolution on consumer protection in online video games (2023),³⁰ the European Parliament refers to the protection of minors in several places: for example, it calls on video game developers and distributors to ensure that games aimed at minors respect children's rights, including privacy, targeted advertising, and manipulative practices. Children need to have the same level of protection when playing video games as they have under the digital services legislation.

The Digital Education Action Plan (2021–2027)³¹ sets out a shared vision for high-quality, inclusive, and accessible digital education in Europe, with the aim of supporting the adaptation of Member States' education and training systems to the digital age. The document underlines that, among other things, a reliable digital education ecosystem requires secure platforms that ensure continuous data protection and comply with ethical standards. In addition, everyone needs to have a basic understanding of new technologies, including AI, to participate safely in their use and to be aware of issues related to data protection, privacy, and children's rights.

The European Media Action Plan³² focuses on the news media sector, audiovisual entertainment, video games, and innovative solutions such as virtual reality experiences. It points out that the latest European legislation contributes to ensuring greater responsibility of all media players, including online platforms, to protect minors, among others, to use media services responsibly and better equip them to deal with the dangers of online violence and disinformation.

The European Union's Security Union Strategy³³ warns that continued steps are needed to combat illegal content online. Fundamental threats to citizens, such as child sexual abuse, are increasingly taking place in digital environments, with the proliferation of child sexual abuse material on the Internet. This calls for concrete action. Companies must be able to continue their work to detect and remove child pornography online, and the damage caused by this kind of material calls for a framework setting out clear and permanent obligations to tackle the problem. The Commission will also start preparing sector-specific legislation to better tackle online child sexual abuse.

The European Union's Action Plan on Human Rights and Democracy (2020–2024)³⁴ has a specific heading on promoting human rights and democracy using digital technologies. It stresses the importance of capacity building and other support to enable national authorities to develop and implement relevant international legislation effectively, including for the protection of children online.

The Recommendation on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online (2014)³⁵ sets out measures to keep minors away from online gambling. The document

30 European Parliament, 2023.

31 European Commission, 2020b.

32 European Commission, 2020c.

33 European Commission, 2020d.

34 European Parliament and the Council, 2020.

35 European Commission, 2014.

states that minors may not be given the opportunity to play on gambling sites. To prevent access to such sites, Member States must promote the inclusion of links to parental control programs. They must also ensure that commercial communications for online gambling services do not induce minors to view gambling as a natural element of their leisure time activities. Commercial communications should also carry a clear “no underage gambling” message indicating the minimum age below which gambling is not permissible.

The European Union’s Youth Strategy (2019–2027)³⁶ recognises that there are young people who do not have access to the Internet and digital technologies, or the skills to use them. The document aims to ensure that parents, carers, and teachers are equipped with media and digital literacy skills. Young people also have problems in checking the accuracy and reliability of information. They need training to navigate the media, and to recognise and report online hate speech and discrimination. It must be ensured that young people are able to engage in tolerant and non-violent online dialogue.

3.2. Acts of the European Union

The EU has recently been quite active in the legislative field to regulate the digital space, in particular, the Internet and social media. Given that the extraordinary pace of ICT technological development can have a significant impact on the physical and mental health of minors, child protection rules are also often included in these legal acts. Accordingly, the Digital Services Act (DSA) of 19 October 2022,³⁷ which is one of the most comprehensive EU-level legal instruments on the subject, also contains child protection provisions, including stipulations in the Recitals. The DSA also includes rules that are not specifically child protection-focused, but which also protect children.

Recital 64 of the DSA states in general terms that, under certain conditions, providers of online platforms should temporarily suspend their relevant activities in respect of the person engaged in abusive behaviour. However, service providers can also take stricter measures for child sexual abuse content, among other things. The protection of children is specifically addressed in Recital 71 and Article 28, which require platform providers to take appropriate and proportionate measures to protect minors. Furthermore, they may not present advertisements based on profiling using the recipient of the service’s personal data if the service’s recipient is a minor. According to Recital 80, large online platforms are required to assess four categories of systemic risks. Among these, the DSA mentions the dissemination of child sexual abuse material and the risks to their rights. Article 34 requires service providers to identify, analyse, and assess systemic risks related to their services, such as their design, operation, and use, with care. For the systemic risks identified, they must

36 Council of the European Union and the Representatives of the Governments of the Member States, 2018.

37 European Parliament and the Council, 2022.

put in place risk mitigation measures in accordance with Article 35. These include measures to protect children's rights, such as age verification, parental control, and other tools that allow minors to flag abuse.

Among the legal provisions that protect children as well as other users – given the importance of the protection to be provided – it is worth mentioning Recital 22 of the DSA, which requires the service provider to act without delay to remove any unlawful activity or content upon becoming aware of it. Service providers may become aware of the illegal nature of content through own-initiative investigations and notifications, among other things. In the latter context, Article 16 also explicitly requires service providers to supply a means of reporting illegal content in an easily accessible, user-friendly, and electronic way. The removal of content must respect the right of the recipient of the service to freedom of expression and information. Consequently, if the service provider detects, for example, content that is harmful to minors, it must remove it while notifying the user, and must give reasons for its decision, in accordance with Article 17. In addition, under Article 20, users must be given the right to appeal against the decision and the possibility of out-of-court dispute settlement under Article 21. Article 18 obliges the provider to report suspected offences to the law enforcement authorities of the Member State concerned if it has information that gives rise to a suspicion that a criminal offence has been, is being, or is likely to be committed that threatens the life or safety of a person or persons.

The Audiovisual Media Services Directive (AVMS Directive),³⁸ amended in 2018, strengthens the protection of children from harmful content and inappropriate commercial communications. Under Paragraph 1 of Article 6a, Member States shall ensure that audiovisual media services that are likely to impair the physical, mental, or moral development of minors are accessed only in such a way that minors cannot normally hear or see them. This can be ensured, for example, by measures such as the choice of broadcasting time or the use of age verification devices, proportionate to the harm the programme may cause. The most harmful content must be subject to the strictest measures. Similar rules are set out in Article 28b for video-sharing platform providers. Accordingly, Member States shall ensure that these service providers respond appropriately to protect minors from programmes, user-generated videos, and audiovisual commercial communications that could harm their physical, mental, or moral development. The Article also protects the public in general from content that is a criminal offence to distribute, among other things, with child pornography as an example.

Article 9 of the AVMS is intended to ensure that audiovisual commercial communications accompanying children's programmes do not emphasise the benefits of foods and drinks that are harmful to children. In general, audiovisual commercial communications must not cause physical, mental, or moral harm to minors, must not encourage minors to buy or hire products or services by exploiting their inexperience or credulity, must not directly encourage minors to persuade their parents or others

38 European Parliament and the Council, 2010.

to buy the advertised product or service, must not exploit the special trust minors place in their parents, teachers, or other persons, and must not unreasonably show minors in dangerous situations. In addition, audiovisual commercial communications relating to alcoholic beverages must not specifically target minors. Article 22 prohibits television advertising and teleshopping for alcoholic beverages specifically aimed at minors and stipulates that it must not depict minors consuming alcohol. In relation to audiovisual media services or programmes that are sponsored, Article 10 states that the sponsorship of children's programmes, or the showing of the sponsorship logo during children's programmes, may be prohibited. Article 11 of the AVMS also prohibits product placement in children's programmes. Under Article 20, the transmission of children's programmes may be interrupted by television advertising once for each scheduled period of at least 30 minutes. The transmission of teleshopping is prohibited during children's programmes.

Article 1 of the Directive on combating the sexual abuse and sexual exploitation of children, adopted in 2011,³⁹ establishes minimum rules concerning the definition of criminal offences and sanctions in sexual abuse and sexual exploitation of children, child pornography, and solicitation of children for sexual purposes. It also introduces provisions to strengthen the prevention of those crimes and the protection of their victims.

Recital 38 of the General Data Protection Regulation (GDPR),⁴⁰ adopted in 2016, which has set the standard for the security of the digital space, states that children's personal data deserve special protection. This specific protection applies to the use of data for marketing purposes or for the creation of personality or user profiles. According to Recital 65, the data subject should have the right to have their personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, where a data subject has withdrawn their consent, or objects to the processing of personal data concerning them, or where the processing of their personal data does not otherwise comply with the GDPR. That right is relevant where the data subject has given their consent as a child and later wants to remove such personal data, especially on the Internet. The Regulation also lays down specific provisions for children in relation to information society services. According to Article 8, the processing of personal data in relation to such services offered directly to children shall only be lawful with the consent of the parent in the case of a child under the age of 16.

A relatively recent piece of EU legislation is the General Product Safety Regulation, adopted by the Council in April 2023,⁴¹ which states that children also have the right to safe products. Importantly, online sales are also covered by the Regulation.

39 European Parliament and the Council, 2011.

40 European Parliament and the Council, 2016.

41 European Parliament and the Council, 2012.

The Unfair Commercial Practices Directive⁴² sets out specific provisions for children in relation to advertising. Its Recital 18 states that it is appropriate to include in the list of unfair practices a provision protecting children from direct exhortations to purchase. According to Point 28 of Annex I to the Directive, the inclusion in an advertisement of a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them shall qualify – among others – as a misleading commercial practice. The Commission has published guidelines for the interpretation and application of the Directive in a communication in 2021.⁴³

3.3. Case Law of the Court of Justice of the European Union

The CJEU plays a central role in the development of European integration. It ensures that EU laws are interpreted and applied in the same way in all Member States, and that both Member States and institutions respect EU law. Its case law has a fundamental impact on the legal systems of the Member States, and its judgments are a source of law. Previous CJEU decisions on the subject can therefore also be of great help in interpreting the legal issues that arise in the digital space, which is incompletely codified due to the constant and rapid technological changes. In the context of the protection of children in the digital space, the following judgments can be highlighted.

The case of *Dynamic Medien v. Avides Media*⁴⁴ concerns the legality of German labelling restrictions on imported DVDs and video cassettes that had already been subject to such inspections in the UK, then an EU Member State. To ensure the free movement of goods within the EU, double regulation of goods is generally prohibited. However, the CJEU concluded in the case that German controls on age-limit labelling lawfully restrict the free movement of goods within the EU, given that they are aimed at protecting children. The CJEU referred to the Convention on the Rights of the Child, which encourages States Parties to protect children from harmful information in the media.⁴⁵

A significant decision was made in relation to IP addresses in the *La Quadrature du Net and Others v. Premier ministre and Others*⁴⁶ case. In its judgment, the CJEU pointed out that the analysis of the IP address constitutes a serious interference with the user's right to respect for privacy under Article 7 of the Charter of Fundamental Rights, and their right to the protection of personal data under Article 8. However, it adds that account must be taken of the fact that, where an offence is committed online, the IP address might be the only means of investigation, enabling the person to whom that address was assigned at the time of the commission of the offence to be identified. This

42 European Parliament and the Council, 2005.

43 European Commission, 2021c.

44 ECJ, C-244/06 *Dynamic Medien Vertriebs GmbH v. Avides Media AG*, judgment of the Court (Third Chamber) of 14 February 2008.

45 European Union Agency for Fundamental Rights, Council of Europe, 2015, p. 30.

46 ECJ, joined Cases of C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v. Premier ministre and Others*, judgment of the Court of Justice (Grand Chamber) of 6 October 2020.

finding was cited by the CJEU two years later in *G.D. v. The Commissioner of the Garda Síochána and Others*,⁴⁷ and in the *SpaceNet case*,⁴⁸ in relation to child pornography.

According to the GDPR, one of the cases of lawful processing of personal data is when it is necessary for the purposes of the legitimate interests pursued by the controller or a third party. However, processing is unlawful where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, where the data subject is a child. The CJEU interpreted this exception in *Meta Platforms and Others v. Bundeskartellamt*⁴⁹ as follows. The GDPR requires a balancing of conflicting rights and interests, depending on the specific circumstances of the case. It is for the referring (national) court to make this assessment. It is apparent from the very wording of Article 6 of the GDPR that it is necessary, in such a balancing exercise, to pay particular attention to the situation where the data subject is a child. According to Recital 38, children merit specific protection regarding the processing of their personal data. Such specific protection must apply to the processing of personal data of children for the purposes of marketing, or creating personality or user profiles, or offering services aimed directly at children.

In the main proceedings of *Booky.fi Oy v. Kansallinen audiovisuaalinen instituutti*,⁵⁰ a Finnish online store distributed audiovisual programmes on physical media without an indication of the age limit and content information required by the applicable Finnish law. The Finnish National Audiovisual Institute ordered the company to remedy the omission. However, the company did not comply, claiming that the classification had already been conducted in another Member State. The case was eventually referred to the Finnish Supreme Administrative Court. The Court referred the case to the CJEU for an interpretation of whether the obligation to classify and label programmes in accordance with the age limits set out in the Act goes beyond what is necessary to achieve the aim pursued by the Act, of protecting children.

The CJEU has ruled as follows. The fundamental treaties do not preclude the legislation of a Member State which, with the objective of protecting minors, requires that audiovisual programmes recorded on a physical medium and marketed via an online store have previously been the subject of an inspection procedure and classification, according to age limits, and corresponding labelling in accordance with the law of that Member State, including where those programmes have already been the subject of a comparable procedure and of comparable classification and labelling in application of the law of another Member State, provided that the legislation is appropriate

47 ECJ, C-140/20, *G. D. v. the Commissioner of A Garda Síochána and Others*, judgment of the Court (Grand Chamber) of 5 April 2022.

48 ECJ, joined Cases of C-793/19 and C-794/19, *Bundesrepublik Deutschland v. SpaceNet AG, Telekom Deutschland GmbH*, judgment of the Court (Grand Chamber) of 20 September 2022.

49 ECJ, C-252/21, *Meta Platforms and Others v. Bundeskartellamt*, judgment of the Court (Grand Chamber) of 4 July 2023.

50 ECJ, C-662/21, *Booky.fi Oy v. Kansallinen audiovisuaalinen instituutti*, judgment of the Court (Tenth Chamber) of 23 March 2023.

for securing the attainment of that objective and does not go beyond what is necessary to attain it.

4. Conclusions

There are several documents dealing with the protection of children in the digital space at both international and EU level. These include soft law material (strategies, reports, action plans, guidelines, etc.), international conventions promulgated by law, EU legal acts, and judgments of the ECtHR and the CJEU.

At the international level, the activities of UNESCO, UNICEF, and the UN Human Rights Council are prominent in the adoption of soft law documents, which provide useful guidance in the field of child protection. The international conventions that have been transposed into the legal systems of the States Parties have a more significant impact. This category includes, among others, the UN Convention on the Rights of the Child, which provides general protection for children, the Lanzarote Convention on the protection of children against sexual exploitation, and the Convention on Cybercrime, which criminalises child pornography.

The EU has produced many soft law documents on child protection. In particular, these include the EU Strategy on the Rights of the Child, which also focuses strongly on digital safety, the Digital Compass 2030, the new strategy for a better internet for kids, and the EU Security Union Strategy, which can contribute to protecting children online in the coming years.

However, the EU documents adopted as legal acts already provide protection on a normative basis. According to the DSA, very large online platforms must implement risk mitigation measures (such as age verification) to address risks to children's rights. The Directive on combating sexual abuse, sexual exploitation of children, and child pornography sets minimum rules concerning the definition of criminal offences and sanctions. Additionally, the GDPR states that children merit specific protection concerning the processing of their personal data.

In the context of international court practice, in most relevant cases, the decisions are not explicitly aimed at establishing a violation of the rights of the child in the digital space. However, the connection of the act to the digital space is part of the (offline) violation of the rights of the child(ren). Most decisions in EU case law do not contain findings on the protection of children in the digital space in the substantive part but rather in other parts of the judgments.

Bibliography

- Chatzinikolaou, A. (2018) ‘Benedik v Slovenia: Police need a court order to access subscriber information associated with a dynamic IP address. Strasbourg Observers’, *Strasbourg observers*, 1 June [Online]. Available at: <https://strasbourgobservers.com/2018/06/01/benedik-v-slovenia-police-need-a-court-order-to-access-subscriber-information-associated-with-a-dynamic-ip-address> (Accessed: 18 January 2024).
- Council of Europe (1989) ‘European Convention on Transfrontier Television’, *European Treaty Series No. 132*. [Online]. Available at: <https://rm.coe.int/168007b0d8> (Accessed: 18 January 2024).
- Council of Europe (2001) ‘Convention on Cybercrime (ETS No. 185)’, *Council of Europe Treaty Series No. 201*. [Online]. Available at: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (Accessed: 18 January 2024).
- Council of Europe (2007) ‘Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse’ [Online]. Available at: <https://rm.coe.int/1680084822> (Accessed: 18 January 2024).
- Council of the European Union and the Representatives of the Governments of the Member States (2018) ‘Resolution of the Council of the European Union and the Representatives of the Governments of the Member States meeting within the Council on a framework for European cooperation in the youth field: The European Union Youth Strategy 2019–2027’ [Online]. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:42018Y1218\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:42018Y1218(01)) (Accessed: 18 January 2024).
- EU Law Live (2021) ‘ECtHR: Grand Chamber judgement concerning children abuse in Bulgarian orphanage and procedural obligations under Article 3 ECHR’, *EU Law Live*, 2 February [Online]. Available at: <https://eulawlive.com/ecthr-grand-chamber-judgement-concerning-children-abuse-in-bulgarian-orphanage-and-procedural-obligations-under-article-3-echr> (Accessed: 18 January 2024).
- European Commission (2014) ‘Commission Recommendation 2014/478/EU of 14 July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online’ [Online]. Available at: <https://op.europa.eu/en/publication-detail/-/publication/f84fa393-0f01-11e4-a7d0-01aa75ed71a1/language-en> (Accessed: 18 January 2024).
- European Commission (2020a) ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: EU Strategy for a more effective fight against child sexual abuse, COM/2020/607 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0607> (Accessed: 18 January 2024).

- European Commission (2020b) ‘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. COM/2020/624 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0624> (Accessed: 18 January 2024).
- European Commission (2020c) ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: Europe’s Media in the Digital Decade: An Action Plan to Support Recovery and Transformation, COM(2020) 784 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0784> (Accessed: 18 January 2024).
- European Commission (2020d) ‘Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions: The EU Security Union Strategy, COM(2020) 605 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605> (Accessed: 18 January 2024).
- European Commission (2021a) ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: The EU Strategy on the Rights of the Child, COM/2021/142 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0142> (Accessed: 18 January 2024).
- European Commission (2021b) ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions – 2030 Digital Compass: the European way for the Digital Decade, COM/2021/118 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118> (Accessed: 18 January 2024).
- European Commission (2021c) ‘Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market’ [Online]. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229\(05\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)) (Accessed: 18 January 2024).
- European Commission (2022) ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: A Digital Decade for Children and Youth: new strategy for a better internet for kids (BIK+), COM (2022) 212 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0212> (Accessed: 18 January 2024).

- European Parliament, European Council (2005) ‘Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005L0029> (Accessed: 18 January 2024).
- European Parliament, European Council (2010) ‘Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L0013> (Accessed: 18 January 2024).
- European Parliament, European 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’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0093> (Accessed: 18 January 2024).
- European Parliament, European Council (2012) ‘Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023R0988> (Accessed: 18 January 2024).
- European Parliament, European Council (2016) ‘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)’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679> (Accessed: 18 January 2024).
- European Parliament, European Council (2020) ‘Joint Communication to the European Parliament and the Council: EU Action Plan on Human Rights and Democracy 2020–2024, JOIN/2020/5 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0005> (Accessed: 18 January 2024).
- European Parliament, European Council (2022) ‘Regulation (EU) 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’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065> (Accessed: 18 January 2024).
- European Parliament (2023) ‘European parliament resolution of 18 January 2023 on consumer protection in online video games: a European single market approach (2022/2014(INI))’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023IP0008> (Accessed: 18 January 2024).

- European Union Agency for Fundamental Rights, Council of Europe, 2015.
- Fengchun, M., Wayne, H. (2023) *Guidance for generative AI in education and research*. Paris: UNESCO; <https://doi.org/10.54675/EWZM9535>.
- Human Rights Guide (2012) ‘Case Rothe v. Austria’, *Human Rights Guide*, 4 December [Online]. Available at: <https://www.zmogausteisiugidas.lt/en/case-law/rothe-v-austria> (Accessed: 18 January 2024).
- Milkaitė, I. (2023) ‘Open minds, open hearts: Macatė v. Lithuania on restricting and labelling a children’s book that depicts same-sex families in a positive light’, *Strasbourg Observers*, 31 March [Online]. Available at: <https://strasbourgobservers.com/2023/03/31/open-minds-open-hearts-macate-v-lithuania-on-restricting-and-labelling-a-childrens-book-that-depicts-same-sex-families-in-a-positive-light> (Accessed: 18 January 2024).
- UNESCO (2020) *Education for sustainable development: A roadmap*. Paris: UNESCO; <https://doi.org/10.54675/YFRE1448>.
- UNESCO (2022) *Transforming technical and vocational education and training for successful and just transitions: UNESCO strategy 2022–2029*. Paris: UNESCO [Online]. Available at: https://unevoc.unesco.org/pub/unesco_strategy_for_tvete_2022-2029.pdf (Accessed: 18 January 2024).
- UNESCO (2023) *World Youth Skills Day 2023: Empowering youth for a sustainable future*. Bonn: UNESCO-UNEVOC International Centre for TVET [Online]. Available at: <https://unevoc.unesco.org/i/883> <https://unevoc.unesco.org/i/883> (Accessed: 18 January 2024).
- UNICEF (2019) *Every child learns: UNICEF education strategy 2019–2030*. New York: UNICEF [Online]. Available at: <https://www.unicef.org/media/59856/file/UNICEF-education-strategy-2019-2030.pdf> (Accessed: 18 January 2024).
- UNICEF (n.d.) ‘Guidelines for journalists reporting on children’ [Online]. Available at: <https://www.unicef.org/eca/media/ethical-guidelines> (Accessed: 18 January 2024).
- United Nations (n.d.) ‘Annual reports of the Human Rights Council – Special Rapporteur on the sale and sexual exploitation of children’ [Online]. Available at: <https://www.ohchr.org/en/special-procedures/sr-sale-of-children/annual-reports-human-rights-council-and-general-assembly> (Accessed: 18 January 2024).
- United Nations General Assembly (1989) Convention on the Rights of the Child, New York, 20 November, General Assembly resolution 44/25 [Online]. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> (Accessed: 18 January 2024).
- United Nations General Assembly (2000) ‘Optional protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict, General Assembly Resolution A/RES/54/263’ [Online]. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-involvement-children> (Accessed: 18 January 2024).

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 project² 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 Today⁴

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. Research¹² 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 Protection¹⁶

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 Programme¹⁸ 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 legislation²² 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 environment²⁷ 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 strategy²⁹ 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).

Children in Digital Age – Croatian Perspective

Hrvoje LISIČAR

ABSTRACT

Today, it is difficult to imagine life without digital technology and the Internet. They have become an integral part of our everyday lives, especially the lives of children and young people. Children use the Internet for learning, entertainment, communication, creativity and to express themselves. Digital technology and especially the Internet gives them access to a variety of information, services and opportunities that can enrich their childhood, development, and well-being. However, the digital environment also carries numerous challenges and risks for children's rights. Children can be exposed to violence, abuse, exploitation, explicit sexual content, hate speech, misinformation and disinformation, various other types of manipulation and other harmful content on the Internet. Children may also face violations of their right to privacy, dignity, identity, and participation in the digital environment. They can be discriminated against or excluded because of lack of access, equipment, skills or support to use digital technology. Therefore, it is important to ensure that children have the same rights and protections in the digital environment as they have in our everyday lives. This implies respect, exercise and protection of all children's rights established by the Convention on the Rights of the Child and other international and national documents. It also implies involving children in decision-making and policies that affect their lives in the digital age. In Croatia, there are numerous actors and initiatives that deal with issues of children's rights in the digital environment. Among them are state bodies, non-governmental organisations, academic institutions, the media and the business sector. They carry out various activities, such as education, prevention, counselling, research, advocacy and monitoring, to promote and protect children's rights in the digital world. This chapter aims to provide an overview of children's internet use in Croatia; this includes the legal framework for the protection of children's rights in the digital age together with definitions of legally relevant terms in national legislation as well as some examples of judicial practice and discussion about rights to privacy, to be forgotten, to access to information, to education, to be safeguarded from abuse, to freedom of expression, and to be heard.

KEYWORDS

children's rights, digital environment, children and the Internet, digital age, information society and children, social media, audiovisual medial services, video-sharing platforms, media literacy

Hrvoje LISIČAR (2025) 'Children in Digital Age – Croatian Perspective' in Halász, Cs. (ed.) *Children in Digital Age*. Miskolc-Budapest: Central European Academic Publishing, pp. 105–128. https://doi.org/10.71009/2025.csh.cida_6.



1. Definitions and Taxonomic Rationale

To better protect children in a digital environment, one of the key prerequisites is to understand how children use the Internet. In recent years, numerous studies have been carried out on this topic, involving children of different age groups and with a different approach. Most of them were carried out by non-governmental organisations and academic institutions.

The most recent research was done in 2022 by the Safer Internet Centre Croatia¹ in cooperation with public and private institutions. This research included 2016 respondents in 21 high schools in all regions of Croatia. The results of this research were presented at the Cyber Security Conference in October 2022.² The main goal of this research was to deepen the knowledge about the risky behaviours of 1st and 3rd class high school students (aged 14 and 16) in the online environment and to find out to what extent high school students are exposed to harmful content and sexual harassment in the online environment. The research showed that 37.6% of high school students spend five or more hours a day on the Internet, of which more than 10% spend 10 or more hours on the Internet, and 56% of high school students use the Internet more than they did before the COVID-19 pandemic. They spend the most time on networks that offer video content, such as YouTube, Instagram, Snapchat, and TikTok, and 5.4% of respondents said they also use the social network Tinder. Furthermore, with regard to inappropriate content, as many as 20% of high school students witnessed or experienced sexual harassment on the Internet in the last year. Almost 50% of respondents state that they witnessed their peers share sexual content on a group chat, profile, or forum. More than 30% state that their peers secretly take photos of naked, half-naked, or inappropriately dressed people or during certain sexual acts and share them on the Internet. Additionally, more than 30% of the respondents testify that their peers share photos of sexual content with people their age. Almost 30% of high school students state that they would not report sexual harassment on the Internet because they are worried that they would be blamed for it. The research also showed that 41.2% of young people were sexually assaulted at least once. They were more often girls (48.7%), than boys (34%). However, every fourth child has experienced some form of sexual abuse on the Internet and most of the respondents first encountered sexual content on the Internet around the age of 13.

Other research with a focus on children and their interaction with information technology in a digital world also showed similar results. National research on children's safety on the Internet titled "HR Kids Online"³ conducted by Society for Communication and Media Culture in cooperation with government agencies,

1 Safer Internet Centre Croatia: making the Internet a good and safe place [Online]. Available at: www.csi.hr (Accessed: 21 January 2024).

2 Ramljak et al., 2022.

3 Cibodi et al., 2020.

non-governmental organisations (NGOs), and the private sector in 2017 included 1,017 children aged 9–17 years and the parent who has more insight into the child's online practices. The key results of the research showed that children most often access the Internet via smartphones. Almost 50% of children aged 9–11, 66% of children aged 12–14, and 75% of children aged 15–17 can access the Internet whenever they want or need to. Every fourth child aged 9–14 and every third child aged 15–17 are completely or mostly concerned about their privacy on the Internet. Every 10th child aged 15–17 accepts all friend requests from other people on social networks. Simultaneously, almost 25% of children of that age look for new friends or contacts on the Internet every week. Every fifth child aged 9–17 completely or mostly does not know how to change privacy settings, for example, on social networks. Almost every third child aged 9–17 has communicated online with people they have not met in person in the last year (from the time of the survey). This was done by every 10th child aged 9–11, every fourth child aged 12–14, and almost every other child aged 15–17. When the last time something upset or bothered them online, more than half of children aged 9–17 closed the app, one in three children blocked the person so they could no longer contact them, one in four children ignored the problem, and one in five children changed their privacy settings. More than half of children aged 9–17 have received a hurtful or inappropriate message. More than 33% of children aged 9–11, almost 50% of children aged 12–14, and almost 75% of children aged 15–17 had received such a message. Children who spent more time on the Internet during the week and over the weekend received such messages more often. Almost 66% of children aged 9–17 have seen sexual photos or a film of a naked person on the Internet in the past year, without intending to see them. This was experienced by 75% of children aged 9–11, more than 65% of children aged 12–14, and almost 65% of children aged 15–17.⁴ Research also showed that parents often talk about internet activities with younger groups of children. Concurrently, parents monitor the online activities of younger groups of children much more often than they do teenagers' activities, but also give younger children advice on what to do if someone is harassing them online.

The results of both surveys clearly show that digital technology and the Internet are a large part of the everyday life of children in Croatia. Research also shows the extent to which children are at risk when using the Internet and the need for better regulation when it comes to internet communication, harmful content, and a better level of protection for children's rights in the digital environment. For this reason, we continue to review the current legislative framework for children's rights in Croatia's digital environment.

When considering the legal framework for the protection of children in the digital environment in Croatia, we must consider all legal areas and laws that protect children and their rights. As a party of the Convention on the Rights of the Child (hereafter,

4 EU Kids Online istraživačka mreža, 2020.

“Convention”),⁵ Croatia is among those countries that have undertaken the obligation to ensure the protection of children’s rights and freedoms. Respecting, protecting, and promoting those rights and freedoms is a task that derives from the Croatian Constitution,⁶ and the well-being of children depends on achieving those goals. Art. 62 of the Croatian Constitution stipulates that the state protects motherhood, children, and youth, and creates social, cultural, educational, material, and other conditions that promote the realisation of the right to a dignified life. Furthermore, art. 63 of the Constitution imposes the obligation on the parents to raise, support and educate children but also gives them the rights and freedoms to decide independently about their children’s upbringing. Finally, Art. 64 stipulates that it is everyone’s duty to protect children. Furthermore, for protection of children in a digital environment, other relevant legislation is the Family Act (FA),⁷ Primary and Secondary School Education Act (PSSEA),⁸ Criminal Code (CC),⁹ Electronic Media Act (EMA)¹⁰ and its regulations, Media Act (MA),¹¹ General Data Protection Regulation (GDPR)¹² together with an Act on implementation of the General Data Protection Regulation (AIGDPR),¹³ and the Electronic Commerce Act (ECA).¹⁴

The FA includes provisions relating to protection of children’s right to education¹⁵, right to freedom of expression and the right to be heard¹⁶, and the right to access to information¹⁷. These rights are also guaranteed by the provisions of the PSSEA. The FA does not provide an exact definition of the term “child”; on the contrary, the limits of the term are only mentioned when FA says that an adult is someone who has reached the age of 18. Similarly, the concept of “parent” is also not defined in the FA; instead, the FA talks about motherhood and paternity, which can be determined by presumption, recognition, or court decision¹⁸.

5 United Nations (1989) UN Convention on the Rights of the Child, New York, 20 November 1989; The Republic of Croatia has been a party since the beginning of its state independence based on the succession notification (Official Gazette of the SFRJ, No. 15/1990, Official Gazette, International Agreements, No. 12/1993, 20/1997).

6 Constitution of the Republic of Croatia (Official Gazette No. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 76/10, 85/10, 5/14).

7 Family Act (Official Gazette No. 103/15, 98/19, 47/20, 49/23, 156/23).

8 Primary and Secondary School Education Act (Official Gazette No. 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 126/12, 94/13, 152/14, 7/17, 68/18, 98/19, 64/20, 133/20, 151/22, 155/23, 156/23).

9 Criminal Code (Official Gazette No. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23).

10 Electronic Media Act (Official Gazette No. 111/21, 114/22).

11 Media Act (Official Gazette No. 59/04, 84/11, 81/13, 114/22).

12 European Parliament and the Council, 2016.

13 Act on implementation of the General Data Protection Regulation (Official Gazette No. 42/18).

14 Electronic Commerce Act (Official Gazette No. 173/03, 67/08, 130/11, 36/09, 30/14, 32/19).

15 Arts. 84 and 94 of the FA.

16 Art. 86 para. 1 of the FA.

17 Art. 86 para. 2 of the FA.

18 Arts. 58 and 60 of the FA.

The CC includes provisions relating to protection of privacy and personal data and especially provisions relating to the right to be safeguarded from the abuse in the digital environment. It also provides a definition of the term “child” in Art. 87 para. 7, where a child is defined as a person who has not reached the age of 18. In this regard, the Juvenile Courts Act¹⁹ in art. 2 defines a minor as a person who has reached the age of 14 at the time of committing the crime but has not reached the age of 18.

With regard to the media literacy and protection of children from inappropriate or harmful content, especially on video-sharing platforms (VSP), the EMA governs the obligations of the providers of those services and imposes special obligations for the purpose of protecting children’s rights.

Relating to the protection of privacy, specifically protection of personal data of the children and their processing, erasure, consent, and transparency in a digital environment the relevant provisions can be found in the GDPR and AIGDPR.

Finally, the ECA defines all digital services, including digital media and social networks as information society services, and establishes the rules and conditions under which such services must be provided. According to Art. 2 para. 2 of the ECA, information society services are services that are provided electronically for a fee at the individual request of the user, and in particular internet sales of goods and services, offering data on the Internet, advertising via the Internet, electronic search engines, and the possibility of searching for data and services that are transmitted via an electronic network, mediate access to the network or store user data.

There is no special law in Croatia that specifically regulates the protection of children against digital harm; each of the aforementioned laws covers a certain area of protection of children’s rights or provision of services to children in the digital environment for the purpose of a further comprehensive analysis. Therefore, it is necessary to take them all into account.

2. Legal Protection of Children’s Rights on the Internet

2.1. The Right to Privacy and the Right to Be Forgotten

With the development of information and communication technologies, the right to privacy, as a fundamental human right, has become a key topic for everyone who uses these technologies, and this especially refers to the protection of children’s privacy in the digital environment. Notably, the right to privacy consists of at least five discrete dimensions: physical and mental integrity, decisional autonomy, personal identity, informational privacy, and physical/spatial privacy.²⁰ This right is inextricably linked to other rights such as freedom of expression, safeguard from abuse, and access to information. In the context of online environments where personal data has become a valuable asset, it is important to impose safeguards to protect informational privacy

19 Juvenile Courts Act (Official Gazette No. 84/11, 143/12, 148/13, 56/15, 126/19).

20 See: Tobin and Field, 2018, p. 554 for an extensive discussion.

of every user and especially children, as they require specific protection with regard to their personal data because they may be less aware of the risks, consequences, and safeguards concerned and of their rights in relation to the processing of personal data. Children's right to informational privacy is their right to have their personal information, communication, and activities protected from arbitrary or unlawful interference by others. This right is based on the recognition that children are entitled to respect for their dignity, autonomy, and identity, and that privacy is essential for their development and well-being.

As in other European Union (EU) member states, in the Republic of Croatia, children's right to privacy as well as their right to be forgotten is protected primarily by the GDPR. This is an EU regulation that aims to protect the personal data of individuals, especially children, who are considered vulnerable and less aware of the risks and consequences of sharing data online. Processing of data is usually a very broad term that can be categorised into three groups: data given, data observed, and data that is derived or inferred.²¹ Therefore, it is essential to consider all provisions of the GDPR and of the AIGDPR relating to the processing of children's personal data.

Art. 6 of the GDPR protects children's personal data by requiring a lawful basis for processing it, such as consent, contract, legal obligation, vital interest, public interest, or legitimate interest including special provisions with regards to children's consent when it comes to information society services. This refers to the processing of data that can be classified into all three groups mentioned above. Art. 8 of the GDPR stipulates that children under 16 cannot give valid consent by themselves, and need the authorisation of the holder of parental responsibility if that age limit is not set lower by the member states. Croatian AIGDPR in art. 19 sets the limit of 16 years of age for valid consent given by a child to information society services, the same as the GDPR. As the holder of parental responsibility is not defined under the GDPR, it must be determined by consulting the Croatian FA. This restriction of children's rights to give valid consent is also reflected in the FA's Art. 95 para. 4, which determines that the holder of parental responsibility has the right, duty, and responsibility to supervise the child in his socialising with other people, such as via communication on social networks, or other forms of electronic communication, and to prohibit him from socialising and communications that are not in accordance with the child's well-being.

For a child or holder of parental responsibility to give valid consent to the processing of personal data, they must be able to make an informed decision. This implies fulfilling the fundamental principle of transparency according to Art. 5 para. 1a of the GDPR as well as all other principles. The principle of transparency contributes to the awareness of children and holders of parental responsibility about the nature, risks, consequences, safeguards, and their rights with regard to the processing of personal data and ultimately protection of their informational privacy. In accordance with art. 12 of the GDPR, this includes the provision of information about what is done

21 Cf. Caglar, 2021, p. 6.

with their personal data, being open about the possible risks that can be connected to the processing, what the safeguards are and letting them know about their rights if they want to object to the processing. This must be done in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed to a child.

In cases where the child or holder of parental responsibility withdraws his consent to the processing of personal data, or the consent is invalid (not given or acquired in accordance with a law), or the personal data are unlawfully processed or no longer necessary in relation to the purposes for which they are collected or otherwise processed, Art. 17 of the GDPR stipulates that everybody has the right to erasure of their personal data. Rec. (65) of the GDPR specifically refers to the cases where the data subject is a child and explains that the right to be forgotten is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the Internet. Other provisions of the GDPR that contribute to the protection of children's privacy, such as the implementation of the principles of accountability and security, can also be considered in this context, but given the limited scope of this analysis, we do not address this further.

In addition to GDPR and AIGDPR as a *lex generalis* regulation dealing with the protection of informational privacy, children's privacy in a digital environment is also protected by other regulations. In connection with media publication of children's personal data, both offline and online, the Croatian MA especially protects children by stipulating in Art. 16 para. 1 that the media are obliged to respect the privacy, dignity, reputation, and honour of citizens, especially children, youth and families, regardless of gender and sexual orientation. It is forbidden to publish information that reveals the identity of a child if it endangers the well-being of the child. Furthermore, this provision is strengthened by the EMA's Art. 24 para. 5 when it comes to all forms of electronic media (audiovisual media services, electronic publications, and VSP); it stipulates that it is not permitted to publish information that reveals the identity of a child under the age of 18 involved in cases of any form of violence, regardless of whether he is a witness, a victim, or the perpetrator or if the child has attempted or committed suicide, nor to provide details of the child's family relationships and private life. Furthermore, when personal data are processed by the VSP, Art. 96 para. 8 of the EMA stipulates that minors' personal data collected or otherwise obtained by the VSP's service providers during the establishment and application of an age verification system for VSP service users in relation to content that could harm minors' mental, physical, or moral development or while providing parental control systems that are under the end user's control in terms of content that could harm minors' physical, psychological, or moral development, such data may not be processed for commercial purposes, such as direct marketing, profile creation, or targeted behavioural advertising.

The right to privacy and right to seek just pecuniary compensation for violating this right is also guaranteed by the Civil Obligations Act²² in Art. 1100 para. 1, which stipulates that in the event of violation of personality rights, the court shall, where it finds that this is justified by the seriousness of the violation and circumstances, award a just pecuniary compensation, irrespective of the compensation for material damage and in the absence of the latter.

Finally, children's right to privacy is protected and enforced by the Croatian CC. Section XIV of the CC deals with criminal offences against privacy. This section pertains to protection of privacy for all citizens, including children. In connection with the use of information technology, Art. 142 para. 1 of the CC pertains to violation of confidentiality of letters and other shipments and stipulates that whoever opens someone else's parcel, letter, telegram, electronic mail, or any other means of correspondence without authorisation, or violates their confidentiality in another way, or keeps, conceals, destroys, or hands over someone else's closed parcel or letter, telegram, electronic mail, or any other means without authorisation correspondence, will be punished by imprisonment for up to one year. Furthermore, with regard to misuse of recordings of sexually explicit content, Art. 144a para. 1 of the CC stipulates that whoever abuses a relationship of trust and without the consent of the recorded person makes available to a third person a recording of sexually explicit content that was recorded with that person's consent for personal use and thus violates the privacy of that person, shall be punished by imprisonment for up to one year. This also pertains to anyone who uses a computer system or in another way creates a new or modifies an existing recording of sexually explicit content and uses that recording as a real one, thereby infringing a person's privacy on that recording. If the recording has become available to a large number of persons through a computer system or network or in another way, the perpetrator shall be punished by imprisonment of up to three years²³. Finally, with regard to protection of personal data, art. 146 (1) of the CC stipulates that whoever collects, processes, or uses the personal data of persons contrary to the conditions specified in the law, will be punished by a prison sentence of up to one year. If the offence is committed against a child contrary to the conditions specified in the law, punishment shall consist of a prison sentence of up to three years. It is also important to note that this criminal offence is prosecuted *ex officio*.

2.2. The Right of Access to Information and the Right to Education

When considering children's right of access to information and the right to education and their realisation in the digital environment, it is worth noting that children have the right to seek, receive, and impart information and ideas of all kinds, through any media of their choice, in a language they understand and without any censorship or

22 Civil Obligations Act (Official Gazette No. 35/05, 41/08, 125/11, 78/15, 29/18, 126/21, 114/22, 156/22, 145/23, 155/23).

23 Art. 144a para. 3 of the CC.

interference. To achieve this goal, it is necessary to create a safe environment and protect children from potentially dangerous and harmful content.

The Croatian FA determines children's right to education as a fundamental part of parental care. According to art. 92 (1) 2 of the FA, the content of parental care includes among other obligations an obligation for the upbringing and education of the child. Furthermore, Art. 94 para. 3 of the FA stipulates that parents have the duty to take care of their child's all-round, regular, and further education and encourage his artistic, technical, sports, and other interests according to their possibilities. In addition to the obligations of parents, the right to access information and the right to education in a digital environment is also guaranteed in educational institutions. The Croatian PSSEA sets out the main goals and principles of upbringing and education in educational institutions; in Art. 4 para. 1 of the PSSEA, one of the main goals is the obligation of educational institutions to ensure that students acquire basic (general education) and professional competencies, and are trained for life and work in a changing socio-cultural context according to the requirements of the market economy, modern information and communication technologies, and scientific knowledge and achievements. Furthermore, art. 4 in paragraph (2) 10 stipulates that everyone has the right to education. Children have the right to an influx of information or content, which is transmitted in an objective, critical, and pluralistic manner, based on modern scientific and educational standards important for the complete and harmonious development of their personality. The task of the public school system is to be neutral and balanced and to enable the child to exercise this right.

With regard to children's rights to access to information in a digital environment, it is important to consider the Croatian EMA as one of the most important laws addressing children's access to electronic media content. The EMA represents the implementation of Audiovisual Media Services Directive (AVMS Directive)²⁴ into the Croatian legislative framework that contains provisions pertaining to VSPs and regulates electronic publications²⁵ in Croatia. With regard to securing a safe environment for children when accessing electronic media and user-generated content published on a VSP, thus enabling them to access the information freely without endangering their well-being and development, Art. 24 paras. 2–3 and Art. 96 para. 1 of the MA stipulates that it is prohibited in electronic publications and on VSPs and other audiovisual media services to publish content that can seriously harm the physical, mental, or moral development of minors, especially those that include gratuitous violence. Furthermore, para. 3 of Art 24. stipulates that content of audiovisual media services, electronic publications, and user-generated content published on a VSP that is likely to harm the physical, mental, or moral development of minors must not be published, except when the provider ensures, by selecting the broadcast time, age verification

24 European Parliament and the Council, 2018.

25 According to Art. 3 para. 6 of the EMA, electronic publications are editorially designed, produced, or collected media content published via the Internet by electronic publication service providers for the purpose of public information, entertainment, or education.

tools or any other technical measure, that minors in the transmission area will not, as a rule, hear or see it. With regard to audiovisual commercial communications related to games of chance, audiovisual media services and radio programmes that are broadcast in unencoded form, the provider is obliged to ensure that they are preceded by an audible warning or that they can be recognised by means of visual symbols for the entire period of their duration. VSPs also have special obligations with regard to the protection of minors determined by Art. 96 para. 7 of the EMA, which consists of an obligation to establish and apply an age verification system for users of video-sharing platform services in relation to content that could harm minors' psychological, physical, or moral development; the obligation also pertains to the establishment of parental control systems that are under the control of the end user in terms of content that could harm minors' physical, psychological, or moral development. The obligation extends to ensuring effective media literacy measures and tools and raising user awareness of these.

In relation to parental responsibilities and children's right to access to information it is also important to consider an Ordinance on protection of minors in electronic media (OPMEM).²⁶ This ordinance prescribes the technical measures and obligations of the providers of audiovisual media services, electronic publications, and VSPs when they publish media content that is likely to harm or that may seriously harm minors' physical, mental, or moral development. According to art. 15 of the OPMEM, on-demand audiovisual media services (e.g. Netflix, HBO+, and others) have an obligation to establish the conditional access system that prevents minors from accessing, seeing, or hearing content that is likely to harm their physical, mental, or moral development and to categorise²⁷ such content with visual symbols that are clearly visible in their catalogue and during every announcement or recommendation of such content. With regard to the same type of content published in electronic publications, art. 17 of the OPMEM stipulates that providers must implement age verification systems or other technical means to prevent minors from freely accessing such content. In case of content that is likely to impair minors' physical, mental, or moral development that is used for educational, artistic, scientific, or informative purposes, providers are obliged to ensure that such content is easily recognisable using warnings describing the possible harmful nature of the content. Similarly, Art. 16 of the OPMEM regulates the obligations of the VSPs with regards to user-generated content. VSPs that are under the jurisdiction of Croatia have an obligation to undertake appropriate measures regarding the user-generated content that can or is likely to harm minors' physical, mental, or moral development (through conditional access, an age verification system, parental guidance, and reporting and flagging content).

26 Ordinance on the Protection of Minors in Electronic Media (Official Gazette No. 106/22).

27 Art. 8 of the OPMEM prescribes the categorisation of all electronic media content into three groups – Category 12 for content suitable for children older than 12, Category 15 – for children older than 15 and Category 18 – content not suitable for children.

2.3. The Right to Be Safeguarded From Abuse

Children's right to be safeguarded from abuse in a digital environment and especially in connection to the use of social networks and other forms of digital communications in the Croatian legislative framework is primarily guaranteed by the CC. Protection from intrusive behaviour is guaranteed by art. 140 of the CC, where paragraph (1) stipulates that whoever persistently and over a long period of time follows or stalks another person or tries to establish or establishes unwanted contact with him or intimidates him in another way and thereby causes him anxiety or fear for his safety or the safety of persons close to him, shall be punished by imprisonment of up to one year. Paragraph (2) of the same article stipulates that if this offence was committed in relation to a close person, a person with whom the perpetrator was in an intimate relationship, or a child, the perpetrator shall be sentenced to imprisonment of up to three years. Although this provision deals with intrusive behaviour generally, in criminal cases that are committed in a digital environment using information and communication technologies, this provision is also applicable. In close connection to the criminal offence of intrusive behaviour is also the criminal offence of enticing children to satisfy sexual needs, which is prohibited and regulated by Art. 161 para. 1 of the CC. This article stipulates that an adult who commits a criminal offence against a person under the age of 15, with the intention that he or another person commits a criminal offence of sexual abuse of a child under the age of 15²⁸, or exploits children for pornography²⁹ or pornographic shows³⁰, through the information of communication technologies or in another way, proposes a meeting with her or another person and who takes measures to ensure that meeting takes place, shall be punished by imprisonment from six months to five years. Another safeguard for children in general but which also applies to a digital environment is set out in Art. 163 of the CC; it regulates exploitation of children for pornography, which in paragraph (1) stipulates that whoever entices, recruits, or encourages a child to participate in the filming of child pornography or who organises or facilitates its filming, shall be punished by imprisonment from one to 10 years. Furthermore, paragraph (2) of the same article stipulates that whoever unauthorisedly records, produces, offers, makes available, distributes, disseminates, imports, exports, obtains for himself or another, sells, gives, shows, or possesses child pornography or consciously accesses it through information and communication technologies shall be punished with the penalty from paragraph (1) of this article. Paragraph (3) stipulates that whoever, by force or threat, deception, fraud, abuse of power, or difficult position or dependency, forces or induces a child to record child pornography, shall be punished by imprisonment from three to 12 years. Paragraph (4) of this article pertains to the devices used and content created and stipulates that special devices, means, computer programs, or data intended, adapted, or used for committing or facilitating the commission

28 Art. 158 of the CC.

29 Ibid., Art. 163.

30 Ibid., Art. 164.

of the criminal offence referred to in paragraphs 1, 2, and 3 of this article shall be confiscated, and pornographic material that was created by the commission of the criminal offence referred to in paragraphs 1, 2, and 3 of this article will be destroyed. Paragraph (5) of this article, which pertains to children's possession or production of such materials, also stipulates that a child shall not be punished for the production and possession of pornographic material depicting himself or himself and another child if they themselves produced the material and possess it with the consent of each of them and exclusively for their personal use. Finally, paragraph (6) provides a definition of child pornography as material that visually or otherwise depicts a real child or child that does not exist in reality or person who looks like a child in real or simulated sexually explicit behaviour or which depicts the genitals of a real child or a realistically depicted non-existent child or person who looks like a child for sexual purposes. Materials depicting the genitalia of a real child or a realistically depicted non-existent child or person who looks like a child, and which have artistic, medical, or scientific significance are not considered pornography in the sense of this article.

Similar to previous articles of the CC, Art. 164 of the CC regulates the criminal offence of exploiting children for pornographic shows. Paragraph (1) of this article stipulates that anyone who lures, recruits or encourages a child to participate in pornographic performances shall be punished by a prison sentence of one to 10 years. Paragraph (2) of this article pertains to material benefit obtained from this criminal offence and stipulates that whoever makes money from pornographic performances in which a child participates or otherwise exploits a child in a pornographic performance, shall be punished by imprisonment from one to 12 years. According to paragraph (3), whoever forces or induces a child to participate in a pornographic performance by force or threat, deception, fraud, abuse of authority, or a difficult position or dependent relationship, shall be punished by imprisonment from three to 12 years. In connection to online environments, paragraph (4) stipulates that anyone who watches a pornographic performance live or via means of communication shall be punished with imprisonment from paragraph (1) of this article if he knew or should have known that a child was participating in it. Furthermore, in connection with devices used to commit this criminal offence paragraph (5) regulates that special devices, means, computer programs, or data intended, adapted, or used for committing or facilitating the commission of the criminal offence referred to in paragraphs (1), (2), and (3) of this article shall be confiscated, and pornographic material that was created by the commission of the criminal offence referred to in paragraphs (1) and (2) of this article will be destroyed. Finally, paragraph (6) provides a definition of a pornographic performance as the live presentation or through communication means of a real child or a realistically depicted non-existent child or a person who looks like a child in real or simulated sexually explicit behaviour or the sexual organs of a real child, a realistically depicted non-existent child or a person who looks like a child for sexual purposes.

Introducing children to pornography in any way including in digital environments is also a criminal offence regulated by Art. 165 of the CC. Paragraph (1) stipulates

that whoever sells, presents, shows, or publicly exhibits, through a computer system, network, or media for storing computer data or otherwise makes accessible writings, images, audiovisual content, or other objects of pornographic content to a child under the age of 15, or shows pornographic material to a child under the age of 15, shall be punished by imprisonment from six months to five years. According to paragraph (2), items, special devices, means, computer programs, or data intended, adapted, or used to commit or facilitate the commission of this criminal offence shall be confiscated, and pornographic material shall be destroyed. Finally, paragraph (3) of Art. 165 defines pornography as material that visually or otherwise depicts a person in real or simulated sexually explicit behaviour or that depicts human sexual organs for sexual purposes. Materials that have artistic, medical, or scientific significance are not considered pornography in the sense of this article.

Finally, as a *lex generalis* for all information society services, ECA with its Art. 5a para. 1 stipulates that a court or other competent government body can take measures to limit the freedom to provide information society services to service providers based in the member states of the EU. This would apply to the service provider that causes or threaten to cause damage, and at the request of an authorised person whose rights have been violated. Limit to the freedom to provide service is imposed for the purpose of prevention, research, detection, and prosecution of perpetrators of criminal acts, including the protection of minors and the fight against all forms of incitement to hatred due to race, gender, religion, or nationality and violations of individual persons' human dignity.

2.4. The Right to Freedom of Expression and the Right to Be Heard

The right to freedom of expression is guaranteed by Croatian Constitution in Art. 38, which pertains to freedom of the press and other means of communication, freedom of speech and public performance, and the free establishment of all institutions of public communication. Furthermore, as a personal right of every child, the FA in Art. 86 determines the child's right to express his opinion. According to paragraph (1) of this article, parents and other persons who take care of the child are obliged to respect the opinion of the child in accordance with his age and maturity. Paragraph (2) stipulates that in all proceedings in which a decision is made about a child's right or interest, the child has the right to learn the important circumstances of the case in an appropriate manner, to receive advice and express his opinion, and to be informed of the possible consequences of respecting his opinion. The child's opinion is taken into account in accordance with his age and maturity. Although this provision of paragraph (2) is primarily focused on proceedings like parental custody, adoption, and other formal proceedings, it can also be applicable in cases where consent of holders of parental responsibility is required for children's use of some digital services or for the processing of the child's personal data if they are younger than 16.

Media literacy is one of the key prerequisites for being able to exercise the right to freedom of expression and to protect other rights like privacy or the right to receive information. The right to information reflects the need of children and young people

to search for information and thus fulfil themselves as individual beings acting in society.³¹ The child has the right to freedom of expression and that right must, regardless of frontiers, include the freedom to seek, receive, and disseminate information. For this reason, it is important that the state requires the promotion of media and digital literacy. With regard to electronic media and VSPs, this is mandated in art. 11 of the EMA, where the activity of publishing audiovisual and radio programmes and the content of electronic publications is of public interest when the programmes relate, among other things, to media literacy. Moreover, art. 19 of the EMA stipulates that the Council for Electronic Media must promote programmes for the development of media literacy knowledge and skills. Art. 96 para. 7 of the EMA imposes similar obligation on providers of VSPs and stipulates that while providing their services they must provide effective measures and tools for developing media literacy and raising user awareness of these measures and tools.

3. Overview of Relevant Case Law

Regarding children's right to be safeguarded from abuse, specifically in relation to Art. 163. of the CC that pertains to the exploitation of children for pornography, we can refer to the case on which the Supreme Court of the Republic of Croatia has ruled.³² In this case, the defendant appealed to the Supreme Court based on the verdict of the first-instance criminal court, by which he was sentenced to three years and six months in prison for exploiting a child for pornography and publishing the content on Facebook. Based on the facts of the case, the ruling of the court in the first instance and rules on the possibility of mitigating the sentence of Arts. 48 and 49 of the CC, the Supreme Court changed the sentence to two years and six months of imprisonment and one year and three months of a conditional sentence. The facts of the case are as follows. The accused was in an intimate relationship with the injured party whom he met through Facebook. The injured party stated on her Facebook profile that she was 24 years old. During the proceedings before the court of the first instance, it was proven that the defendant knew that the injured party was a minor, because during the relationship he congratulated her on her 15th birthday via Facebook and found out during the relationship that she was attending high school. After a quarrel with the injured party, the defendant posted a photo on his Facebook that he had taken, in which the injured party satisfied him orally. The defendant claimed that he did it out of anger, but after a few minutes he regretted posting the photo and removed it from his Facebook profile. The Supreme Court confirmed the decision of the lower court on the correct determination of the existence of the criminal offence of exploiting a child for pornography from Art. 163 CC. Moreover, evidence trying to prove the claim that the accused did not know that she was a minor was rejected. Owing to the defendant's

31 See: Koren, 2005, p. 268 for an extensive discussion.

32 Supreme Court of the Republic of Croatia, case No. Kžzd 38/2019-9.

youth, his behaviour during the proceedings, his confession, and his lack of prior convictions, the Supreme Court decided to partially reduce the sentence imposed by the lower court.

In connection with the use of social networks by children for the exchange of explicit content, we can refer to the decision of the County Court in Bjelovar.³³ In this case, the County Court decided on the appeal of two minor defendants filed against the decision of the Municipal Court in Bjelovar,³⁴ which had imposed a sanction on the defendants in the form of an educational measure ordering them to be involved in the work of humanitarian organisations or in work of communal or environmental significance so that in during a six-month period, the minor J.P. worked 80 hours, and the minor T.R. 30 hours, in a way that did not interfere with their education. In this case, J.P. encouraged T.R. to ask a minor classmate to send him a photo of her naked body via Facebook profile, which she did. After receiving the photo the defendants published a photo in a Facebook group. As her face was not shown in the photo, in the appeal against the decision they claimed that it was not the injured party (M.K.) but instead a generic photo from the Internet. The court carefully analysed the evidence and established that the photo in question indeed shows the injured minor party M.K., which she herself confirmed. During the trial it was also established that the defendants forwarded the photograph in question to other students in the class, clearly stating that it was the injured minor M.K. Their actions constituted the dissemination and display of child pornography according to art. 163 of the CC, which was clear when taking into account the text that accompanied the publication of the photo, that read: ‘Would you have sex with her?’ The court also determined that the case in question was not about the exploitation of children for pornography according to art. 163 of the CC, as the injured party M.K. confirmed that she sent the photo of herself voluntarily, due to sympathy that she felt towards T.R. Bearing in mind the defendants’ age, the seriousness, danger, and frequency of the criminal offences (no prior record), as well as their previous behaviour, and the fact that they expressed regret and embarrassment over the event in question, the County Court confirmed the first-instance court’s assessment and decision.

Next, the case law represents the protection of children’s right to privacy in electronic media. In this case the County Court³⁵ in Pula decided to reject an appeal against the verdict of the Municipal Civil Court in Zagreb,³⁶ which found that children’s right to privacy was violated by publishing an article in an online news portal. The Civil Court ruled in favour of the minor plaintiffs J.K. and J.K. and awarded damages in the amount of HRK 25,000 (equivalent to EUR 3,500) for each plaintiff, which the publisher must pay. In this case, the publisher posted a newspaper article on an online portal that dealt with the topic of parental custody. The article presented the claims of

33 County Court in Bjelovar, case No. Kžm-3/2018-5, 20 September 2018.

34 Municipal Court in Bjelovar, case No. Km-10/2017-19, 28 March 2018.

35 County Court in Pula, case No. Gž-1407/2017-2, 30 July 2018.

36 Municipal Civil Court in Zagreb, case No. Pn-1070/17-39, 4 August 2017.

the father who was trying to obtain custody of the children and thus presented information about the mental illness of the mother, his ex-wife, and circumstances from family life which, according to his claims, had an extremely negative impact on the children's development. He also complained about social services provided by government institutions. The information provided was very detailed and contained enough elements to enable the unequivocal identification of all those involved, including the minor children. The court found that the newspaper article presented inaccurate and unverified information in an inappropriate manner and that the mother and minor children's right to privacy as well as their honour and reputation were violated. Before the publication of the article, mother was not given the opportunity to state her point of view on the problem described by her ex-husband, that is, to dispute his claims about the family circumstances in which the children lived. The publisher also published a photo of the father along with the published text. The Civil Court found that in the case in question, the article was not an authorised text (in its entirety), and the publisher could not be released from responsibility for damages because he grossly violated the provisions of art. 16 of ZM (which stipulates the protection of children's rights to privacy), by revealing the identity of the children, thereby jeopardising their well-being and privacy. The problem with this decision, as with many other cases involving electronic media and publishing information about minors online is that although both Courts found that the publisher violated the children's right to privacy, they did not order the removal of the content^{37,38} that enables the identification of minors from the online portal; even after seven years, this article is still available online in an unchanged form.

One of the landmark cases with regard to the right to be forgotten is the case decided by the Constitutional Court of the Republic of Croatia.³⁹ In this case, the Constitutional Court annulled the decisions of the County Court in Dubrovnik⁴⁰ and Municipal Civil Court in Zagreb⁴¹ and sent the case back to the Municipal Court to carry out the procedure and decide on the case again. Although this case does not involve minors, it is important for deciding on the capacity to act as a defendant when trying to enforce the right to be forgotten and is certainly applicable in the future if minors seek to exercise the aforementioned right. In this case, the applicant M.M. was trying to exercise his right to be forgotten. He first appealed to the Agency for the protection of personal data in Croatia (AZOP), who rejected his claim as unfounded.⁴² Subsequently, he initiated a lawsuit in a civil court. In the first-instance proceedings,

37 Art. 1047 of the Civil Obligations Act stipulates that upon request, the court can order that appropriate measures be taken to prevent the occurrence of damage or disturbance or to remove the source of danger, at the expense of the owner of the source of danger, if he does not do so himself.

38 Art. 1047 of the Civil Obligations Act anticipates that possibility.

39 Constitutional Court of the Republic of Croatia, case No. U-III-3633/2020, 25 October 2023.

40 County Court in Dubrovnik, case. No. Gž-32/2017-3, 4 March 2020.

41 Municipal Civil Court in Zagreb, case No. Pn-3874/2014-14, 30 November 2016.

42 AZOP, decision No. UP/I-041-02/16-01/16, 567-02/10-16-05, 9. June 2016.

the plaintiff asked the court to order Google Hrvatska d.o.o. (a company registered in Croatia) for the removal of search engine results that displayed links to several texts containing his personal data when his full name was entered. The defendant referred to the lack of capacity to act as a defendant and emphasised his objection that he was not the operator of the internet search engine in question and that the search engine was managed by Google Web Search (Google International LLC), so he was legally and technically unable to respond to the request to remove the link from the search results. The defendant also stated that Google Hrvatska d.o.o. is part of Google Inc., but that there is no direct corporate connection with Google Inc. as the former exclusively promotes and sells advertising space. The first-instance court (Civil Court in Zagreb) accepted the defendant's arguments concerning lack of capacity to act as a defendant and completely rejected the applicant's claim as unfounded. Based on the applicant's appeal, the second-instance court (County Court in Dubrovnik) confirmed the legal interpretation of the first-instance court and also rejected the applicant's appeal as unfounded. Based on the complaint, the Constitutional Court decided that the defendant (Google Hrvatska d.o.o.) in this case is a subsidiary of Google Inc., which is exploiting Google Web Search; Google Inc. is using the defendant in Croatia as an entity to promote and sell advertising space; the defendant is registered in Croatia as a legal entity and develops his activities with an orientation towards entrepreneurs and individuals located in Croatia as a commercial agent of the Google group; promoting and selling advertising space, in which the defendant is engaged in Croatia, represents an important part of the business activity of the Google group and it should be considered closely related to Google Web Search. When it comes to the Internet, "data processing" in the meaning of Directive 95/46 represents displaying/publishing personal data on the website; the defendant has a "business establishment" in Croatian territory and "data processing" is carried out within the advertising and commercial activity of the business establishment on the territory of a member state. Following this reasoning, and contrary to the legal understandings of the first- and second-instance courts, the Constitutional Court decided that the defendant's advertising and commercial activity is an essential part of the Google group's business activity and is closely related to Google Web Search; thus according to Directive 95/46, the defendant has the capacity to be a defendant for data deletion because he has a business establishment in Croatia and performs data processing as part of its advertising and commercial activities.

4. Institutional Protection of Children's Rights

One of the public institutions that is involved in the protection of children's rights on the highest level is the Ombudsman for Children (hereafter, "Ombudsman") and the Office of the Ombudsman for Children. The scope of the Ombudsman's work is set out

in art. 7 of the Ombudsman for Children Act (OCA)⁴³ and includes monitoring the coordination of the laws and other regulations in the Republic of Croatia, concerned with protecting children's rights and interests and the provisions of the Constitution of the Republic of Croatia, of the Convention, and other international documents concerned with the protection of children's rights and interests. Furthermore, the Ombudsman also monitors the fulfilment of the obligations of the Republic of Croatia arising from the Convention and other international documents concerned with the protection of children's rights and interests. Their scope of work also includes the implementation of all regulations concerned with the protection of children's rights and interests of and the violation of their individual rights. It also studies general occurrences and manners of violation of children's rights and interests, including their protection and the violations of their rights in a digital environment. Its task is also to propose undertaking measures intended for the creation of a coherent system of protection and promotion of children's rights and interests and for the prevention of harmful activities jeopardising their rights and interests. Furthermore, it encourages children to express their opinion and it respects their opinion, initiates and participates in public activities aimed at the improvement of their position, and proposes measures to enhance the influence of children in society⁴⁴.

In term of authority, the Ombudsman can warn and give proposals and recommendations in respect to promoting and protecting children's rights and interests. According to Art. 12 of the OCA state administration bodies, local and regional administration units as well as corporations and natural persons have the obligation to cooperate with the Ombudsman and submit reports upon his/her demand, give answers to his/her inquiries, and report immediately, at the latest within a 15-day period, to the Ombudsman on activities performed that concern his/her warning, proposal, or recommendation. The Ombudsman has the right to access all data, information and files concerned with the rights and protection of children, regardless of their level of secrecy. Arts. 14 and 15 of the OCA stipulate that if, during the performance of his/her duties, a child is found to be subject to physical or mental violence, sexual abuse, maltreatment or exploitation, negligence, or careless treatment, he/she will immediately lodge a report about it to the competent General Attorney Office, and warn a competent centre for social welfare suggesting measures for the protection of the rights and interests of the child.

With regard to the online environment, the Ombudsman issued several recommendations pertaining to ensuring the conditions to participate in online classes for all children; protection of children's privacy related to the creation, use, and downloading of photographs; issuing invitations to the media not to publish records of violence among children and young people, and many other activities. Moreover, the Ombudsman actively participates in some of the projects that aim to increase the protection of the children online, such as the project Centre for a safer Internet.

43 Ombudsman for Children Act (Official Gazette No. 73/17).

44 Art. 8 of the OCA.

Another institution that is actively involved in protecting children in a digital environment is the Ministry of the Interior (MI). With its project “Red Button”,⁴⁵ the MI has established a platform (an online application) for reporting illegal internet content (even where the legality is in doubt) that refer to various forms of child exploitation or any form of abuse. This platform provides for reporting sexual abuse and exploitation of a child via the Internet, sexual abuse and exploitation of children in direct contact with the perpetrator, and any other punishable behaviour committed to the detriment of the child (family violence, peer violence, physical abuse, neglect, or violation of the child’s privacy through the Internet). Similarly, abuse can be reported on the platform in the case that a child meets someone online who encourages or forces him/her to talk about intimate matters via a social network or messaging application or asks him/her to meet to have sex, to behave sexually in front of a webcam, to take photos or videos of sex content, or photos of his/her naked body or intimate body parts. The application was launched in 2013, and since then, more than 2,500 reports have been submitted. The application can be used by child/victim or by third party/parent to report online abuse or inappropriate or illegal content on the Internet. The reporting process is divided into steps, where the application guides the user through a set of questions related to the event or with regard to the content that he/she wants to report. After reporting a possible criminal offence, the police will conduct a criminal investigation to find the perpetrator, collect the necessary evidence and other important data, take measures related to the safety and protection of the victim, and inform the state attorney’s office of the findings. If the legal requirements are met, they will arrest the perpetrator and bring him to court and/or propose the imposition of precautionary measures that prohibit him from communicating with the victim. The victim will be informed orally and in writing of the rights that belong to him as a victim of a criminal act. In case of illegal internet content, the police will take appropriate measures to remove the content in question or make it inaccessible to children.

The Council for Electronic Media (CEM), an independent regulatory body for electronic media, is also involved in the protection of children’s rights in the digital environment. Their main task is to promote programmes pertaining to media literacy. As stipulated in art. 19 (1) of the EMA, the CEM has an obligation to promote programmes for the development of media literacy knowledge and skills. They are also obliged to inform the European Commission about the actions taken with regard to those programmes. To fulfil its obligations, the CEM has established a platform to promote media literacy (medijskapismenost.hr). This portal is a platform providing support to everyone who participates in media education, primarily children and young people, but also adults. By doing so, the portal provides a variety of educational materials for teaching media literacy in kindergartens and schools, examples of good practice, advice and recommendations for parents and guardians, information on the impact

45 The application can be found on: <https://redbutton.gov.hr/online-prijava/7> (Accessed: 15 January 2024).

of different types of media and media content and social networks on children and young people, safety on the Internet, the problem of misinformation, and reports on global media and communication trends, as well as policies related to media literacy, media education, and media and digital platforms. The main goal of establishing this platform was for it to become a central place for information about media education, media literacy, policies and trends in the media and audiovisual industry, and to empower parents and all those involved in the education of children to actively seek knowledge and information about media, social networks, and digital platforms and the ways in which they can influence children's development.⁴⁶ The CEM is also involved in many other activities that promote media literacy, for example, organising "Days of media literacy", preparing educational material, and organising education for children.

One of the most prominent initiatives for the protection of children on the Internet is the project "Safer Internet Centre Croatia: Making internet a good and safe place".⁴⁷ The project leader is the NGO Centre for Missing and Abused Children. Although it is an NGO project, it is strongly supported by a number of government institutions that are actively involved, and close cooperation has been established with the Ombudsman, CEM, MI, A1 (telecommunications company), and others. The project's goal is to maintain and improve the work of the Safer Internet Centre, the hotline service for reporting harmful content on the Internet, and the helpline service for children and parents so that they can report harmful content and receive professional help. The above services are free for users.⁴⁸ Similar to the MI project "Red Button", this project enables users to report illegal content on the Internet such as materials depicting the sexual abuse of children; hate speech; visual representations of sex; abused children; trade in children; other forms of child exploitation; racial and other discrimination; or inappropriate chat with children on the Internet.

In the context of strategic planning, the Government of the Republic of Croatia has adopted the "National plan for children's rights in the Republic of Croatia for the period from 2022 to 2026"⁴⁹ together with an "Action plan for children's rights in the Republic of Croatia for the period from 2022 to 2024".⁵⁰ Within the Strategy and Action plan, one of the Government's special objectives is the *systematic support for children in the digital environment* (Special objective No. 4). To achieve this goal, several special implementation measures have been anticipated. Measure No. 1

46 Council for Electronic Media, n.d.

47 Safer Internet Centre Croatia: Making the internet a good and safe place [Online]. Available at: www.csi.hr (Accessed: 21 January 2024).

48 Services can be accessed on the www.csi.hr/hotline where users can report abuse (Accessed: 21 January 2024).

49 National plan for children's rights in the Republic of Croatia for the period from 2022 to 2026 (Official Gazette No. 55/2022).

50 Action plan for children's rights in the Republic of Croatia for the period from 2022 to 2024 [Online]. Available at: <https://mrosp.gov.hr/UserDocsImages/dokumenti/Socijalna%20politika/Dokumenti/Akcijски%20plan%20za%20prava%20djece%20u%20RH%20za%20razdoblje%20od%202022.%20do%202024.%20godine.pdf> (Accessed: 21 January 2024).

is encouraging preventive programmes in the educational system aimed at media literacy. The purpose of this measure is to work on developing media literacy skills, which will help children and young people learn to use the media, analyse and critically question media content, find credible sources of information, protect privacy and personal data, recognise potential harmful media content and inappropriate advertising, recognise and protect themselves from any form of electronic harassment, as well as learn empathy in digital and real world communication. EUR 36,000 is the expected cost for this measure over a period of four years. Measure No 2. is improving the safety and protection of children on the Internet and social networks. The main goals of this measure are to protect children and minors from exposure to illegal and disturbing content, raise the level of knowledge and awareness of children about the dangers of the Internet, and protect their privacy in the context of using the Internet and social networks. To implement this measure, EUR 36,000 have been allocated. Both measures will be achieved through the activities of the CEM.

Finally, media literacy and its promotion is also included in the National curricula for primary school education⁵¹ and high school education.⁵²

5. Summary

According to the data from the Croatian Bureau of Statistics,⁵³ 100% of Croatian children and young people aged 16–24 use the Internet. This is another indicator of how important it is to ensure adequate protection of their rights in the digital environment. The Republic of Croatia, as an EU member state and a state party to the Convention, has implemented numerous legislative measures to protect children's rights in the digital environment. For protecting privacy and the right to be forgotten, the GDPR and AIDDPR are applied, and for protecting the right to access information, measures related to the electronic media and VSP are applied. Furthermore, the Croatian CC has implemented provisions that protect children's rights from abuse, and the provisions of the Council of Europe Convention on Cybercrime⁵⁴ have also been implemented. Finally, by introducing media literacy programmes, an attempt has been made to ensure the right of children to express themselves. In the legislative sense, all the aforementioned laws and their provisions can significantly contribute to the fight for more complete realisation of children's rights in the digital environment. In practical terms and in terms of the laws' implementation, there are certain shortcomings. The first problem is that the rights of children in the digital environment are protected through numerous laws, and it is sometimes extremely difficult to determine which

51 Ministry of Science and Education, 2017a, p. 67.

52 Ministry of Science and Education, 2017b, p. 7.

53 Croatian Bureau of Statistics, 2023.

54 Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185.; Law on the Ratification of the Convention on Cybercrime (Official Gazette, International Agreements No. 09/2022).

law is relevant for a particular case. This is also the case with determining the competent authority for individual cases where children's rights are violated. Another problem is that the development of information and communication technology is not adequately accompanied by legislative activities; it is often the case that considerable time passes from the development of some new service on the Internet that children use extensively to the point of regulation of such services. A good example is the adequate regulation of on-demand audiovisual media services and video-sharing platforms. More than 15 years have passed since the appearance of the first VSPs or on-demand audiovisual media services until the moment when Croatia (based on the implementation of the AVMS Directive) passed adequate legislation regulating the provision of these services. In the meantime, the provision of these services in Croatia was not regulated adequately, so children were not protected in exercising their rights guaranteed by the Convention. The situation is similar regarding social networks. Better protection of children and their rights regarding these services will be implemented in Croatia only after the Digital Services Act⁵⁵ enters into force.

Regarding the institutional protection of children's rights in the digital environment, numerous initiatives exist that have been mainly launched by NGOs. Although the government and regulatory agencies encourage such initiatives and projects, the financial resources that are invested are insufficient to ensure their sustainability. The situation is similar in education. The national curriculum envisages the education of children related to the exercise and protection of their rights in the digital environment, but this education is distributed through numerous subjects, primarily the subjects of the Croatian language (media literacy) and computer science (digital literacy). The curriculum does not envisage a single subject that would introduce children in an adequate and complete way to all the challenges and threats they encounter in the digital environment.

For the purpose of better implementation of the existing legislation, it is necessary to work on the education of judges and other competent persons, especially with getting to know the way in which children use information and communication technology in order to be able to better protect their rights. *De lege ferenda* in general with regard to protection of children's rights in a digital environment, the legislator in Croatia should be more proactive in regulating new information services on the Internet that children use extensively (not waiting for initiatives at the EU level). Information and communication technology and related services are developing extremely fast, and their lack of legal regulation can have extremely negative consequences for children's rights and for society as a whole.

55 European Parliament and the Council, 2022.

Bibliography

- Caglar, C. (2021) 'Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?', *European Journal of Law and Technology*, 12(2), pp. 1–31 [Online]. Available at: <https://ejlt.org/index.php/ejlt/article/view/828/1025> (Accessed: 12 January 2024).
- Cibodi, L., et al (2020) 'Nacionalno istraživanje o sigurnosti djece na internetu HR Kids Online' [Online]. Available at: <http://hrkids.online/prez/EUKidsOnlineHRfinal.pdf> (Accessed: 11 January 2024).
- Council for Electronic Media (n.d.) 'About the portal' [Online]. Available at: <https://www.medijskapismenost.hr/o-nama/> (Accessed: 21 January 2024).
- Croatian Bureau of Statistics (2023) 'Announcement on application of information and communication technologies in households and individuals in 2023' [Online]. Available at: <https://podaci.dzs.hr/media/zlgbxpad/zti-2023-1-2-primjena-informacijskih-i-komunikacijskih-tehnologija-ikt-u-kućanstvima-i-kod-pojedinačica-u-2023.pdf> (accessed: 22 January 2024).
- EU Kids Online istraživačka mreža (2020) 'Results of the EUkids online research: children in a virtual environment', *medijskapismenost.hr*, 10 February [Online]. Available at: <https://www.medijskapismenost.hr/rezultati-istrazivanja-eu-kids-online-djeca-u-virtualmom-okruženju/> (Accessed: 12 January 2024).
- European Parliament, European 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: 12 January 2024).
- European Parliament, European Council (2018) Directive (EU) '2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)' [Online]. Available at: <https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng> (Accessed: 12 January 2024).
- European Parliament, European Council (2022) 'Regulation (EU) 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)' [Online]. Available at: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (Accessed: 12 January 2024).
- Koren, M. (2005) 'Children's human rights: right to be informed', *Dijete i društvo*, 6(2), pp. 267–285.

- Ministry of Science and Education (2017a) 'National curriculum for primary school education' [Online]. Available at: <https://mzom.gov.hr/UserDocsImages/dokumenti/Obrazovanje/NacionalniKurikulum/NacionalniKurikulumi/Nacionalni%20kurikulum%20za%20osnovnoškolski%20odgoj%20i%20obrazovanje.pdf> (Accessed: 22 January 2024).
- Ministry of Science and Education (2017b) 'National curriculum for high school education' [Online]. Available at: <https://mzom.gov.hr/UserDocsImages/dokumenti/Obrazovanje/NacionalniKurikulum/NacionalniKurikulumi/Nacionalni%20kurikulum%20za%20gimnazijsko%20obrazovanje.pdf> (accessed: 26 January 2024).
- Ramljak, T., et al. (2022) 'Online seksualno uznemiravanje i mentalno zdravlje srednjoškolaca u Hrvatskoj rezultati istraživanja DeShame1' [Online]. Available at: https://cnzd.org/wp-content/uploads/2022/10/Lucija-Vejmelka-i-Roberta-Matkovic_deSHAME1-Hrvatska.pdf (Accessed: 17 January 2024).
- Tobin, J., Field, S. (2019) 'Article 16: The right to Protection of Privacy, Family, Home, Correspondence, Honour, and Reputation' in Tobin, J. (ed.) *The UN Convention on the Rights of the Child: A commentary*. Oxford: Oxford University Press, pp. 551–599 [Online]. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/privacy-child/Other-Stakeholders/15-Tobin-J-and-Field-SM-Article-16.pdf (Accessed: 11 January 2024).

Children in Digital Age – Czech Perspective

Lenka Westphalová

ABSTRACT

This paper discusses the various rights of children that may be affected in cyberspace. These are the right to privacy, the right to self-determination, and the protection of personal data. It also seeks to contribute to the debate on the notion of digital adulthood (self-legitimacy). The issue of the child versus the Internet is nowadays vast and wide-ranging; it affects several levels, from criminal sanctions to the private law exercise of parental responsibility and the enabling of self-determination of the child or the protection of the child as a consumer. It also ranges from the proper legal context such as the provision of teaching in schools to systematic solutions at the ministerial level.

KEY WORDS

cyberspace, child rights, privacy, data protection, digital adulthood

1. Introduction

It is necessary to point out that with the wave of “informatisation” of the Czech Republic, unanticipated problems are surfacing, whereas the tools to solve these problems on the part of the wider society, transnational institutions, and above all the state are being strenuously sought. The problem of the relationship of the child versus the Internet is huge and one with a broad-spectrum these days, spanning several levels from the exercise of parental responsibility to the provision of education in schools to systematic solutions at the ministry level.

Considering the time of introduction and further rapid development of the use of the Internet in the Czech Republic, the issue of children’s relationship to the Internet is a very “new” issue. The beginnings of the Internet in the Czech Republic date back to the 1990s. The Internet in the form we know today, which is accessible to young people, only became available around 1997. In that year, the largest internet portal in the Czech Republic – seznam.cz – launched its services. At that time, the Internet was not yet widespread in homes and schools. With the development of internet access, which is connected with the development of services not only of the Internet, but also

Lenka WESTPHALOVÁ (2025) ‘Children in Digital Age – Czech Perspective’ in Halász, Cs. (ed.) *Children in Digital Age*. Miskolc-Budapest: Central European Academic Publishing, pp. 129–151.
https://doi.org/10.71009/2025.csh.cida_7.



the media associated with it (computers, smartphones, tablets, laptops, etc.), there has been a development of services and applications provided to end users such as Skype, Facebook, Twitter, Libimseti, ICQ, and various other chat applications.

2. Definitions

2.1. Cyberspace

Cyberspace is a term introduced by the Cyber Security Act No. 181/2014 Sb. Section (§) 2. Sub-paragraph a) of this Act refers to cyberspace as a *‘digital environment enabling the creation, processing and exchange of information formed by information systems, services and electronic communications networks’*. However, defining the Internet, which is undoubtedly a part of cyberspace, is more challenging, although everyone knows this phenomenon and uses and works with it daily. The Internet does not fall under the definition of a person according to the Civil Code; we cannot even include it in the category of things in the legal sense. The Internet is intangible and uncontrollable. The most understandable of technical definitions is the sense of the Internet as a vast global network that connects computer systems around the world.

Act No. 89/2012 (Civil Code) Art. 2389a regulates that (1) In a contract for the provision of digital content, the provider undertakes to make a thing in digital form (digital content) available to the user for his own use, and the user undertakes to pay remuneration for this. (2) If the use of the digital content requires the authorisation to exercise an intellectual property right, the relevant provisions on licensing shall also apply. This amendment to the Civil Code came into force on 6 January 2023, when, among other things, a new, previously unknown type of contract was introduced, namely, a contract for the provision of digital content. The amendment responds to the development of the digital economy and transposes into the Czech legal system two European directives concerning digital products, namely, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contracts for the provision of digital content and digital services (“Digital Content Directive” or “Directive 2019/770”) and Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC and repealing Directive 1999/44/EC (“the Sale of Goods Directive” or “Directive 2019/771”). Terms and conditions are part of contracts with consumers or other customers. These contracts

are usually concluded in an adhesive manner¹. The terms and conditions regarded as “basic conditions” are set by the service provider without the weaker party (consumer, customer) having a real opportunity to influence the content of these terms and conditions.

Social network is another term whose definition cannot be found in the legal system. A social network may be defined as a computer program or web service that allows people to communicate and share information on the Internet via a computer or mobile phone. For example, according to data available in October 2023, the website [statista.com](https://www.statista.com),² indicates that Facebook is the most widely used social network. Users may create their own profiles, upload photos, create groups and establish friendships. The widely used Messenger, which is used for sending messages, is also a platform linked to Facebook, while YouTube, WhatsApp, TikTok, and Instagram are also other widely used networks.

Digital footprint is a term that includes all data created about a person when using the Internet. It includes websites visited, messages sent and received, and information provided about a person to online services. The footprint may be divided into active and passive. A passive digital footprint is left unintentionally. This includes the search history or IP address. This information may be recorded by internet search engines or web servers. The active component of the digital footprint, however, is created by the user themselves through their deliberate disclosure. It includes sent messages, shared posts or photos. The permanence of the digital footprint is its problematic aspect. In addition to being easy to spread, it is also difficult to remove. However, by leaving such information freely available without the person’s consent, the right to privacy is violated. Therefore, in support of it, natural persons have also been granted the right to be forgotten and deleted. In the first instance, these rights were mentioned in the Judgement of the European Court of Justice No. C-131/12; subsequently they were also legally enshrined in the GDPR regulation, namely, in Article 17. Accordingly, the data subject is entitled to request the erasure of their personal data and the administrator is then obliged to do so without unnecessary delay if the conditions set by the regulation are met.

The following legislation can be mentioned in relation to the Czech regulation of digital services, which were adopted following Regulation (EU) 2022/2065 of the

1 An adhesion contract is a contract in which one party sets all the terms and conditions and the other party only has the option to accept or reject the contract without any real influence on its content. This can be summed up by the phrase “take it or leave it.” Adhesion contracts are effective because they save time, e.g., by using pre-prepared forms, but the party that has no opportunity to influence the terms and conditions finds itself in a weaker position. They are therefore concluded where there is a high number of standardized contracts; from this point of view, it is a rational and economically efficient procedure. However, it may happen that in this way, the stronger contracting party imposes contractual terms that are advantageous for itself and disadvantageous for the other party. The Czech Civil Code regulates the conclusion of adhesion contracts in Arts. 1798–1801.

2 Dixon, 2025.

European Parliament and of the Council of 19 October 2022 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation).

Act No. 480/2004 Coll., on Certain Information Society Services and on Amendments to Certain Acts (i.e. the Act on Certain Information Society Services) regulates the liability and rights and obligations of persons providing information society services and disseminating commercial communications in accordance with European Community law.

Act No 132/2010 Coll., concerning on-demand audiovisual media services and amendments to certain acts (Act on on-demand audiovisual media services) regulates video-on-demand audiovisual media services that take the form of different business and technical models, which are privately binding. Technically, this may be through electronic communications networks or cable distribution (Netflix, Voyo). In the case of an on-demand audiovisual media service, the provider takes editorial responsibility for it and compiles a catalogue of programmes.

Act No. 242/2022 Coll., on the services of video-sharing platforms and amending certain related acts (Act on the services of video-sharing platforms) regulates a video-sharing platform service called Rajče, which is provided by MAFRA, a. s. In the case of this service, the provider does not bear editorial responsibility for it and does not compile a catalogue of video recordings, the arrangement of which is different in law. Although the provider of the latter service determines the arrangement of the video content, this may also be provided by ‘automatic means or algorithms, in particular by displaying, tagging or ranking’, to ‘the general public for the purposes of information, entertainment or education via electronic communications networks’.³

However, from the perspective of copyright law, both services have the legal nature of providing an online content-sharing service if they meet all its conceptual characteristics as defined by copyright law. In this sense, it is significant that the online content-sharing service provider has the private law status of a user of a copyright work, artistic performance, sound recording, sound recording or television and radio broadcast under the Copyright Act. A consumer or customer using an online content sharing service (user of such a service) is a user of protected goods.

2.2. Legal Personality

Legal personality is the ability to possess rights and obligations within the limits of the legal order (Article 15, Sub-section 1 of the Civil Code⁴). The law stipulates that a person has legal personality from birth until death (Article 23 of the Civil Code). It is established that every person has innate natural rights, which may be identified upon reason and feeling alone, and therefore is considered a person. The natural rights associated with human personality may not be alienated and may not be waived; if this does happen, it is ignored.

³ Act No. 242/2022 Sb. Art. 2 para. 1 point a).

⁴ Act No. 89/2012 Sb. of the Civil Code.

After birth, each child shall be registered in the book of births kept by the Register of Vital Records (cf. Article 7 of the Convention on the Rights of the Child⁵). In particular, the name and surname of the child, date of birth, gender, names and surnames of their parents are entered in the Register (Article 14 of the Register of Vital Records Act⁶).

2.3. Legal Capacity

Legal capacity means that a person is a person in their own right (*sui iuris*), that is, they are qualified to acquire rights for themselves through their own legal action and to commit to obligations, that is, to act legally.⁷ Autonomy thus does not belong to everyone, in contrast to legal personality. Furthermore, it is established that every person is responsible for their actions, if they can judge and control them. Legal capacity means, among other things, the basis of a person's delictual liability, that is, the capacity to be a delictual debtor. Based on a person's intellectual and volition maturity, one may distinguish between full capacity and partial capacity.

Full capacity means that a person is capable of fully acquiring rights for themselves through their own legal actions and fully committing themselves to obligations (Section § 15, Sub-section 2 of the Civil Code). As a rule, the law stipulates that a person becomes fully legally capable upon: the age of majority, that is, upon reaching the age of 18⁸.

Before this age, a person becomes fully legally capable upon: recognition of capacity⁹, by entering into marriage; capacity is not lost either by the dissolution of the marriage or by declaring the marriage null and void.

Partial capacity belongs to children who are minors and who have not acquired full capacity yet. Owing to the nature of the matter, they acquire autonomy gradually in relation to their intellectual and volitional maturity. It is different for newborns, for early school age children, and for secondary school students. However, in contrast to historical legislation, the law does not establish any age categories of children, such as children under 7 years, from 8 to 15 years, or over 15 years. The general positive rule is expressed by a rebuttable presumption, according to which it is considered that every minor who has not acquired full capacity is capable of legal actions appropriate in nature to the intellectual and volitional maturity of minors of their age¹⁰. It is an objective concept that admits counterevidence and thus allows the characteristics of a specific child to be taken into account owing to their intellectual and volitional maturity. The law thus guarantees certainty on the one hand, and respects the uniqueness and individuality of each child on the other. The general negative rule states that a minor who has not acquired full capacity is never, regardless of the content of other

5 104/1991 Sb. of the Convention on the Rights of the Child.

6 Act No. 301/2000 Sb. regulating Registries, First and Last Names.

7 Art. 15 Sub-section 2 of the Civil Code.

8 Ibid., Art. 30 Sub-section 1.

9 Ibid., Art. 37.

10 Ibid., Art. 31.

provisions, capable of acting independently in those matters for which even their legal representative would need the permission of the court.¹¹

2.4. Parents and Children

The term “parental responsibility” shall be understood primarily in the form of partial legal and simultaneously moral rules. Furthermore, the child is the weaker party, especially because of their lower age and, as a rule, lower intellectual and volitional maturity. The private law concept of parental responsibility represents an order to take proper care of a child in accordance with the best interest of the child and their well-being, or for the welfare of the child.

The content of parental responsibility is defined as the duties and rights of parents, which (according to Article 858 of the Civil Code) consist of: the care of the child, including in particular the care of their health, physical, emotional, intellectual and moral development; child protection; maintaining personal contact with the child; ensuring their upbringing and education; determining their place of residence; providing their representation; managing their property.

3. Research on Children’s Behaviour in Cyberspace

In the field of research on the behaviour of children in cyberspace, we must mention here the study “Czech children in the cyberworld”, which was carried out in 2019 by the Centre for the Prevention of Risky Virtual Communication of the Faculty of Education of Palacký University in Olomouc and the company O2 Czech Republic.¹² It features research on the risky behaviour of children and adults in online environments carried out by the same team in the years 2015–2018. It is based mainly on the studies called “Risks of Internet Communication IV” (2014) and “Sexting and Risky Acquaintances Made by Czech Children in Cyberspace” (2017) expanded by new findings, which are completely unique in the Czech Republic. The research was funded from the resources of the O2 Czech Republic as part of the so-called contractual research, with neither the public funds of the state nor of the European Union used. An anonymous online questionnaire was chosen as the basic research tool, which was distributed to primary schools in all regions of the Czech Republic. The data collection took place in these schools, from 1 February to 1 May 2019. The statistics software Statistica was used for detailed data evaluation.

A total of 27,177 respondents aged 7–17 from all regions of the Czech Republic took part in the research, with boys constituting 49.83% of the respondents. The average age of the respondents was 13.04 years (median 13, mode 12, variance 4.34). The research group was representative of the age categories of 11–17 years (by age and gender, correlation with the Czech Statistical Office CSO data for 2018). The findings

¹¹ Ibid., Art. 36 Sub-section 1.

¹² Kopecký and Szotkowski, 2019.

of this research included, for example, that children are active consumers of all kinds of content in the online environment: social networks, YouTube videos, e-shops, online encyclopaedias, games, educational sites, news portals, as well as sites with pornographic content. The study found that 23% of children under the age of 13 use social networks, even though they do not meet the minimum age limit for their use.

In the study, the researchers also focused on the issue of active use of a mobile phone by a child. They were interested in whether the child has access to the Internet on their mobile phone without having to be connected to Wi-Fi (e.g. via 3G, 4G, LTE, etc.). More than half of the children (59.1%) confirmed that they have permanent access to the Internet on their mobile phone independently of Wi-Fi. The most common activity reported by children is calling (72%), followed by writing and sending messages via online services (Facebook Messenger, WhatsApp, etc.) (66%). Watching videos on YouTube and writing SMS messages follow.

A comprehensive study¹³ conducted in 25 European countries with 25,000 participants produced the following statistics: 60% of children aged 9–16 use the Internet daily (88 minutes on average) and 59% of these children have a profile on social networks (26% aged 9–10; 49% aged 11–12; 82% aged 13–16). Simultaneously, in the terms of use, no social networks officially allow people under the age of 13 to create an account. Furthermore, in the same European study, 26% of children had their social network profile set to “public” (i.e. accessible to all known and unknown users), 14% reported that their address or phone number was listed on their profile, and 16% admitted that they did not enter their real age on their profile. Additionally, 30% of children surveyed stated they had an online connection with someone they had never met face-to-face, 9% stated they had actually met someone face-to-face with whom they only had had an online connection, 9% stated that they experienced abuse of personal data, 21% reported encountering one or more types of potentially harmful content created by other users, and 6% reported receiving harmful or offensive messages on the Internet. These findings confirm that young children and adolescents use social networks in their daily lives, which may result in the disclosure, misuse, and potential use of personal information. Interestingly, about a third of parents in this European study stated they filter their children’s internet use, while a quarter specifically said they use monitoring tools. With the increasing use of social networks, many users are unknowingly exposed to threats to both their privacy and their security.

4. Protection of Children’s Rights

4.1. Legal Framework in the Czech Republic

The Convention for the Protection of Human Rights and Fundamental Freedoms, which was adopted by the Council of Europe in 1950 in Rome, represents a key source in the wording of the additional protocols regarding protection of human rights in the

13 Livingstone and Haddon, 2011.

Czech Republic (published by Communication No. 209/1992 Sb.). The jurisprudence of the European Court of Human Rights is especially important with respect to family law related to Article 6 protecting the right to a fair trial for everyone; however, above all it is important to Article 8 guaranteeing everyone the right to respect for privacy and family life and Article 14 guaranteeing the prohibition of discrimination. The right to respect for family life is a relative right, that is, it may be subject to restrictions and interventions by the state; if it is not an intervention into the core of this right and further under the conditions that this intervention pursues a legitimate goal, it is carried out by proportionate means and is in accordance with the law.¹⁴

The Convention on the Rights of the Child, adopted by the United Nations in 1989, is dedicated only to children (published by Communication No. 104/1991 Sb., as amended by Communication No. 41/2000 of the Collection of International Treaties). It is a Convention that has an unusually high number of contracting parties, which testifies to its high acceptability not only by almost 200 states of the world but also by the international community as such. This Convention is often called the Magna Carta of Children's Rights. That is why we classify it as a contract of a general nature. It defines a general list of child rights, which may be divided into: protective rights; rights aimed at ensuring the well-being of the child; rights aimed at the liberation of the child, giving children the same rights as adults; the rights of the child in relation to their parents, as regards the self-determination of the child, or their independence in decision-making.

Foreign literature also talks about the three “Ps”, that is, about: protection, provision, participation, or shared decision-making.

Whatever the classification of the rights of the child is, it is necessary to emphasise the application of the Convention to children under the age of 18 if the age of majority is not reached earlier, and especially the main principle of the Convention, which is the interest of the child, or the best interest of the child.¹⁵ The child also has the right to be registered immediately after birth¹⁶ and the right to the care of both parents, or the right not to be separated from them.¹⁷ Finally, anchoring of the child's participation rights shall be underlined, which guarantees the child the status of an active individual who participates in decision-making in their affairs.¹⁸

It should be emphasised here that not all provisions of the Convention are directly applicable in national law (*self-executing*). Therefore, many of them are amended or paraphrased by legal regulation at the level of national law sources. A number of optional protocols have been adopted by the Convention in the matter of children's involvement in armed conflicts (Communication No. 45/2003 of the Collection of International Treaties), the sale of children, child prostitution, and child pornography (Communication No. 74/2013 of the Collection of International Treaties) and the

14 Art. 8, para. 2.

15 Art. 3 of the Convention on the Rights of the Child.

16 Ibid., Article 7.

17 Ibid., Article 9.

18 Ibid., Article 12.

misleading procedure for submission of notifications by individuals to the *Committee on the Rights of the Child* (Communication No. 28/2016 of the Collection of International Treaties). General commentaries were also issued (in particular, Commentary No. 14 of 2013 on the best interests of the child pursuant to Article 3, paragraph 1 of the of the Convention on the Rights of the Child).

The Constitution of the Czech Republic (Constitutional Act No. 1/1993 Sb., as amended), especially in its Preamble, expresses respect for the values of human dignity and human rights in general. It is stipulated that ‘*everyone may do what is not prohibited by law, and no one may be forced to do what is not required by law*’¹⁹ and that fundamental rights and freedoms are under the protection of the judiciary.²⁰ The priority of application of international treaties is also enshrined.²¹

The Charter of Fundamental Rights and Freedoms promulgated as part of the constitutional order of the Czech Republic (under No. 2/1993 Sb.) recognises in its Preamble the natural rights of persons and the generally shared values of humanity. It establishes that all people are free and equal in their dignity and in their rights. Their fundamental rights and freedoms are inherent, inalienable, unlimitable, and irrepealable.²² The charter prohibits discrimination based on sex, religion, social origin, property, or birth.²³ It states that everyone has the capacity to possess rights²⁴ and in particular that everyone has the right to life and that human life deserves to be protected before birth.²⁵ The human dignity of everyone, including children, is also protected and protection against unauthorised interference in private and family life is enshrined.²⁶

The key source of family law is the Civil Code (Act No. 89/2012 Sb., as amended). Part Two of the Civil Code, entitled Family Law, is divided into three chapters devoted to marriage (Chapter I), kinship and affinity (Chapter II), and guardianship and other forms of childcare (Chapter III).

Act No. 561/2004 Sb. (regulating pre-school, primary, secondary, higher vocational and other education, as amended) regulates, among other things, the issue of enrolment and attendance of children in schools in connection with the obligation and right of parents to provide education and training as a component of parental responsibility.

The Act regulating Social and Legal Protection of Children (Act No. 359/1999 Sb., as amended) is the key Act that guarantees the protection of the rights and legitimate interests of the child by the state and sets rules and limits for state authorities. It is a public law regulation, of which it has already been stated that its interpretation

19 Art. 2 para. 4 of the Constitution.

20 Ibid., Art. 4.

21 Ibid., Art. 10.

22 Art. 1 of the Charter of Fundamental Rights and Freedoms.

23 Ibid., Art. 3.

24 Ibid., Art. 5.

25 Ibid., Art. 6 para. 1.

26 Ibid., Art. 10 para. 2.

and application is subject to the principle '*within the limits set by law and in a manner determined by law*' (Article 2, paragraph 2 of the Charter of Fundamental Rights and Freedoms). Social-legal protection is provided by social-legal protection bodies (abbreviated as OSPOD). They are the guardian and representative of the child in proceedings such as decisions about childcare, alimony, and so on. OSPOD looks after children at risk; it is responsible for preventive measures in families, mediates substitute family care, or prepares assessments and recommendations for the court. Regional authorities, municipal authorities of municipalities with extended powers, municipal authorities, the Ministry of Labour and Social Affairs, as well as the Labour Office of the Czech Republic are the bodies of social and legal protection. Social-legal protection is further ensured by municipalities with independent jurisdiction, regions with independent jurisdiction, commissions for social-legal protection of children and other legal entities and natural persons if they are entrusted with the performance of social-legal protection.

4.2. The Principle of the Best Interest of the Child

This principle is also an elaboration of the principle of protection of the weaker party. It is generally recognised that a minor child who is not fully autonomous owing to their age, immaturity, dependence, and so on shall enjoy increased protection not only in connection with private law but also with public law regulation.

International treaties use the broader term "*interest of the child*"; therefore, the term "*the best interest or interests of the child*" is the narrower one. The Civil Code uses the terminology "*interest of the child*" (e.g. Article 792 of the Civil Code) and "*obvious interest of the child*".²⁷

The Convention on the Rights of the Child, as the *Magna Carta* of Children's Rights, stipulates that the child's interest shall be the primary consideration, or the main or primary point of view in any activity concerning children, regardless of who it is carried out by, even the legislator.²⁸ However, from the English text and other translations follows the superlative "*the best interest of the child*".

The best interest of the child belongs to the class of indeterminate, or open legal concepts. It is an objective legal term, which shall, however, be interpreted considering the specific circumstances of the case, that is, especially considering all the family ties of a certain child. The best interest of the child should be considered as the primary, priority, and key principle in all matters concerning the child, as the main rule of interpretation and application.²⁹

Pursuing the best interest of the child should result in the child's well-being. Moreover, the well-being, or welfare of the child should be regarded as the desired goal towards which any activity concerning the child should be directed, with the

27 Art. 793 of the Civil Code.

28 Art. 3 of the Convention on the Rights of the Child.

29 For further analysis of the concept of the best interests of the child, see: Committee on the Rights of the Child General Comment No. 14 (2013) - The best interests of the child as a primary consideration, CRC/C/GC/14; also: Hofschneiderová, 2017.

child's best interest always being pursued. It is possible to consider the well-being of the child as a condition of positive social and mental feeling, that is, not only as a condition where the child lacks nothing but also as a condition accompanied by valuable experiences. This is a concept that is superior to the child's interest.

As already indicated above, children not only are passive objects of the parental responsibility of their parents, other persons, or the state, but they also have participation rights, which, in addition to partial legal capacity³⁰, are guaranteed to children in many places³¹. In any decision-making, their participation rights shall be considered and assessed in relation to the above-mentioned principle of the best interest of the child, even if there is a conflict with the principle of the best interest of the child, or interests of other persons.

4.3. Protecting the Child's Privacy

The right to privacy is one of the indispensable and basic human rights. As such, it is enshrined in the Czech legal system in the Charter of Fundamental Rights and Freedoms of the Czech Republic (Act No. 2/1993 Sb.), specifically in Article 7, which states: 'The inviolability of the person and of privacy is guaranteed'. It may be limited only in cases established by law. Furthermore, the right to protection against unauthorised interference in private and family life is also enshrined in Article 10, paragraph 2 of the Charter of Fundamental Rights and Freedoms. Given that the Charter is a universally valid document, the rights recognised in it naturally also apply to children. This fact is also confirmed by the Convention on the Rights of the Child, which in Article 16 grants children the right to a private life, without interference by other persons, and to be protected against such potential interference. The Commentary to the Convention states that we may either consider the right to private life and family life as separate and distinct rights, or prioritise the right to private life over the family; however, both rights should always be subsumed under the general term "right to privacy". Therefore, the child's privacy must be respected, both by their legal representatives and other persons. The protection of privacy is a right that is not absolute, because to a certain extent, the privacy of a person, including a child, is compromised during any contact with another person who has some information about them. Therefore, every intervention in it may not be considered illegal, and negative consequences may not be drawn from it. However, what is important is to what extent and in what way privacy is affected.

One of the possibilities of encroaching on a child's privacy may be, for example, taking a photo of them, but the photo does not have to be further shared on the Internet for the right to privacy to be violated, which was also confirmed by the ECtHR (European Court of Human Rights) in its judgement in the case of *Reklos and Davourlis v. Greece*. The applicants in this case were parents who had a child born in 1997 at a

30 Art. 31 of the Civil Code.

31 Especially Art. 12 of the Convention on the Rights of the Child, as well as Art. 867 of the Civil Code, specifically Art. 806 et seq. of the Civil Code.

private Greek clinic. After birth, the child was placed in a ward where only medical professionals and clinical staff were to have access. The facility also offered its clients newborn photography services, and as part of this offer, a photographer visited the baby and took a picture of them with their face visible. The parents were not satisfied with this approach, as they did not like the disruption of the sterile environment in which the newborn baby was supposed to be, but especially, they did not give consent to the photography. However, the clinic refused to hand over the negatives of the photographs. The parents therefore filed a claim for damages in the national court, but the claim was dismissed for alleged lack of basis, as was the subsequent appeal. The parents therefore brought the case before the ECtHR, where they filed a complaint about insufficient protection of the right to private life. The final judgement in the case was issued on 15 January 2009. The ECtHR recognised in it that the Greek courts acted in violation of the ECtHR, as they did not take sufficient measures to ensure the protection of the child's privacy, to which a photograph of a person undoubtedly applies. According to the Greek law in force at the time, the consent of the legal representatives was subject not only to possible publication of the photograph but also to its taking. As this consent was not obtained in this case, and moreover, the removal of the negatives, which could later be used against the will of those involved, was refused, the dismissal of the claim for lack of merit constituted a legal error on the part of the court.³²

When applying the right to protect a child's privacy, however, it is probably the most difficult to define it in relation to the child's parent or legal representative. This is where the right to privacy comes into conflict with the parent's right to bring their child up. Strict application of the right to privacy could mean a weakening of the role of parents and thus problems in the functioning of the whole family. There is a generally valid opinion that some aspects of a child's privacy should be respected by parents (e.g. their correspondence), and with increasing age and intellectual maturity, the scope of their privacy should expand. It is about the exercise of parental responsibility, which changes with the growing age of the child.

4.4. Personal Data Protection

Personal data protection is an area that has received more and more attention in recent years, and today there is perhaps no area that is not at least partially affected by this issue. The adoption of the landmark GDPR regulation is the main reason for this.³³ This regulation changed and unified the view on the issue of personal data largely in all sectors and at all stages of their processing, storage, and manipulation. Owing to its wide dispersion, the area of protection of children's personal data was not neglected when creating the GDPR regulation. The importance of protecting

32 *Reklos and Davourlis v. Greece*, Judgement of the ECtHR of 15th April 2009. Complaint No. 1234/05.

33 Regulation (EU) 2016/679, 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).

children's personal data is already emphasised in the Recitals of the Regulation, where point 38 states the following:

‘Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.’³⁴

Furthermore, in the text of the Recitals, specifically in point 58, we also find recommendations for the processing of data relating to children. All information and any communication addressed to the public or to the data subject shall be concise, easily accessible, and easy to understand in a clear and plain language so that children have no problem understanding it. The necessity of transparency and accessibility even for minors is further emphasised in the text of the GDPR regulation itself, namely, in Article 12. Furthermore, it is possible to find a specific arrangement for children's data, for example, regarding the functions of the supervisory authority or the automation of processing. However, the most significant area where a special regulation for children's personal data had to be defined is the area of consent to the processing of personal data, which is necessary for the data to be processed, which is listed in Article 8 of the Regulation. For the ability to express this consent independently, the regulation sets a minimum age limit of 16 years, which the member states may lower based on their own legislation, but not to less than 13 years. Only their legal representative may give consent for children who do not meet this condition. The reason is, of course, that the child is not aware of the risks and consequences that their behaviour and sharing on the Internet may have. It is the duty of the processors of such personal data, such as providers of social networks or computer games, to try to verify as reliably as possible whether the consent was actually given by the legal representative and not by the child themselves.

The regulation faces criticism for the fact that very little attention is paid to the personal data of younger children whose protection is violated by their parents. The regulation, as stated in point 18 of its Recitals, does not apply to the processing of data within the household or of a purely personal nature. Recently, the leakage of personal data through sharing on social networks has been on the rise, while parents often do not even think that they should consider the protection of their children's personal data. This phenomenon is called “sharenting”.³⁵

³⁴ Ibid., p. 9.

³⁵ Citterbergerová, 2023.

4.5. The Child's Right to Self-Determination

Despite the greater or lesser degree of parental responsibility and powers of the parents, the child is an individual personality enjoying all basic human rights and freedoms. For that reason, they also enjoy the right to express themselves if they do not agree with the violation of their privacy, even if the violator is their parent. As already defined above, the sharing of photos and information on the Internet may also be classified as interfering with privacy. For that reason, if a child does not like any of the photos that their parent or anyone else has posted of them, they have the right to ask them to remove the photo. It is not a matter of course that the publisher will comply with the request. The next step may then be to request that the administrator of the social network on which the content was published to remove it. On most popular social networks, including Facebook and Twitter, the function of submitting a request to remove a photo published against the will of the photographed person is available nowadays. For example, with Facebook, the age of the child is crucial. Until the child is 13 years old, Facebook requires that such a request be submitted by the child's legal representative, which excludes requesting the removal of a photo that the parent has added against the child's will.

The United Nations Children's Fund – UNICEF – does not ignore the issue of sharing and children's rights to self-determination regarding the content that is shared about them on the Internet. Therefore, in 2018, it published a publication titled “Children's online privacy and freedom of expression”, which is intended to serve as a kind of guide to the rights of children online, both for themselves and for their parents, as well as for companies that may come into contact with the processing of children's personal data.³⁶

If it is a relationship between a parent and a child, there is an exception in the Czech Republic for the protection of personality. This was also confirmed, for example, by the Supreme Court in its justification of the Judgement No. 30 Cdo 3770/2011. It stated that the child has the right to protection against invasion of privacy by their legal representatives; however, this right is not realised through an action for the protection of personality, but through the means of family law regarding parental responsibility with possible interventions by the court. The fact that these rights are not time-barred or subject to preclusion is also specific to the rights and obligations in the relationship between parents and children. However, although there are theoretical options for a child to legally defend themselves against a parent's invasion of privacy, most experts agree that their possible practical application is very uncertain. Both in society and in legal regulations and case law, the opinion has not been anchored yet that the right to protect a child's privacy is a right independent of their parents' idea of where the boundaries of privacy are and that the parent does not always act only as a “protector and guardian” of this privacy, but also as its violator. The prevailing opinion is that legislative changes will be needed in the coming years, the creation of which will have to consider the change in society towards the digital age.

³⁶ UNICEF, 2018.

4.6. The Right to Be Protected From Abuse

Many minors using social media are unaware of the security risks that exist in these types of communications, including privacy risks, identity theft, malware, fake profiles or social bots, as well as sexual harassment. They also reveal personal and confidential information about themselves, their friends and their relationships, whether by posting photos or directly providing information such as an address or phone number.

Misuse of personal data, shared photos and videos or information is considered a form of cyberbullying. Cyberbullying has taken the place of common physical bullying in today's modern, technological and advanced world. Keith³⁷ defines this phenomenon as follows:

‘Cyberbullying includes the use of information and communication technologies, such as email, mobile phone, pager, text messages, personal websites or social networks, to encourage intentional, repeated, hostile behaviour by an individual or group that is intended to harm others.’

Černá et al.³⁸ describe it as intentional aggressive behaviour carried out either by an individual or by a group through electronic media against a person who cannot defend themselves against attacks at a given moment. Cyberbullying may be just as serious in its effects, if not more serious, than traditional physical bullying. Cyberbullying has the same intention as common bullying in the sense that the aggressor is concerned with harming and damaging the victim using force and taking control or dominance. It differs in the way it is executed, namely, by using modern technologies. Nowadays, children communicate through modern technologies and are thus away from the direct supervision of adults. Therefore, this form of bullying is even more difficult for parents or other adults to detect.

The organisation “People in Need”³⁹ states that, according to research, 15% of pupils and students across Europe have encountered or directly experienced cyberbullying, and 22% of pupils and students have directly experienced it in the Czech Republic. We distinguish between several types of cyberbullying.

One of them, sexting, is becoming a growing problem. Sexting means sending or sharing one's own photos, videos, or texts with sexual or erotic content through modern communication technologies. The user of the social network then places them on the Internet in a profile on the social network or sends them directly via chat, SMS, or email to a specific person. The sending of these photos and texts may take place between peers, partners, or strangers on dating sites and social networks. Children and teen users do not realise that by sending photos and texts with sexual content, they expose themselves to blackmail, abuse, or public ridicule later by the recipient.

37 Keith and Martin, 2005, p. 224.

38 Černá, 2013.

39 People in Need organisation. Program: Více našich webů, 2009.

Sexting with children is considered a criminal offence of spreading child pornography and endangering moral education.⁴⁰ This type of erotically themed content is highly sought after on the Internet. Sexting is also associated with other phenomena, such as blackmail in the form of threatening to send photos to close people.

Another problem is cybergrooming. The goal of cybergrooming is to create false confidence in a child and lure them into a meeting where they can then be sexually abused. Most often, cybergrooming takes place in chat rooms (dating rooms, public chat). Grooming refers in a broader sense to several types of manipulative behaviour.

The very phenomenon of online sexual abuse is not defined in the Acts of the Czech Republic; however, it may be based on, for example, Article 186 of Act No. 40/2009 of the Criminal Code regulating the crime of sexual coercion. This is defined as ‘forcing to sexual intercourse, masturbation, exposure or other comparable behaviour using violence, threats of violence or other serious harm’. Article 202 of the Criminal Code regulating the crime of seduction for sexual intercourse, while the perpetrator offers a child a payment, advantage, or benefit in exchange for sexual intercourse, masturbation, exposure or other behaviour for the purpose of sexual satisfaction of the perpetrator is also of importance here. For example, Article 193 of the Criminal Code regulating the abuse of a child to produce pornography or Article 193b of the Criminal Code regulating establishing illicit contacts with a child, which primarily includes personal meetings between an adult and a child are other relevant provisions.

Child pornography of course, existed before the creation of the Internet. It is not possible to say unequivocally whether the advent of the Internet has boosted the demand for child pornography and expanded the existing market, or whether it is merely satisfying the market in new ways that would certainly exist even without cyberspace. However, the Internet provides an environment for the dissemination of child pornography and the creation of an expanding market for its consumption. It allows offenders to easily produce, view, store, and distribute child pornography. The Internet also serves as a means of communication between perpetrators and acts as an intermediary for contact with potential victims. Child pornography is regulated in the Criminal Code as a ban on the production and other handling of child pornography⁴¹, dissemination of pornography⁴², and abuse of a child to produce pornography⁴³.

40 Spreading pornography according to Section (§) 191 of the Criminal Code, production and other handling of child pornography according to Art. 192 of the Criminal Code, seduction to sexual intercourse according to Art. 202 of the Criminal Code, jeopardising the education of a child according to Art.201 of the Criminal Code, abusing a child for the production of pornography according to Art.193 of the Criminal Code and establishing illicit contacts with children according to Art.193b of the Criminal Code (Act No. 40/2009 Sb. of the Criminal Code).

41 Art. 192 of the Criminal Code.

42 Ibid., Art. 191.

43 Ibid., Art. 193.

5. Regulation of Digital Platforms

In simple terms, it may be said that the means of communication are currently being transformed (from ordinary forms of communication to online communication), which creates pressure to adapt legislation in many areas. For the area of social networks, it is true that these digital platforms are increasingly beginning to fulfil the function of a kind of new public space, which is effectively managed by them (especially in the form of content regulation). However, public space (in its ordinary “offline” meaning) is traditionally associated with a certain form of public law regulation, or with a certain public interest.

The growing importance of social networks then represents a clear challenge for the concept and protection of the rights of individuals in this new space (especially freedom of expression), and the related question (form and degree) of state interference in relation to social networks. The regulation of content carried out by social networks does not, however, seem to consist only of the fulfilment of legal obligations or the application of certain business models. In recent years, influence on the content of social networks clearly motivated by public interest may also be noted. The rules of social networks regulating freedom of speech following the spread of misinformation regarding the COVID-19 disease may be a recent example of this effect.

By its very nature, the public interest should not be an individual interest, but the interest of a certain social group, or a social (or potentially even societal) interest. Sometimes, in this context, we also talk about general interest. When it comes to social networks, there are many levels of public interest. A priori, the public interest in the context of social networks may be identified with the interest of their users, that is, the public. The protection of legitimate (legal) interests of social networks is also undoubtedly a dimension of public interest (or one of the potentially conflicting public interests). After all, social networks themselves (such as so-called online or digital platforms) may be understood as a “product” of public interest in the form of technical development. However, the fundamental question is who should promote the public interest in the context of social networks. At the moment, one may identify clear ambitions of the most influential social networks to regulate their content (also) for the sake of protecting the public interest, without simultaneously dealing with cases that result from a certain legal obligation of the social networks.

6. How Parents Can Protect a Child from the Pitfalls of the Internet By Exercising Parental Responsibility

Within the concept of so-called digital parenting, an active parent is the most important actor who shall participate most significantly in the prevention of negative phenomena associated with Internet abuse. Digital parenting is simply a concept of education in which the parent actively supports the development of their child's

information and communication literacy but also develops other components of their personality (especially social skills, critical thinking, media literacy, etc.). The main recommendations for parents are to be interested in children and their activities on the Internet from an early age, especially in the case of young children, to technically restrict children's access to the Internet, and to possibly monitor their activities. It makes no sense to prevent children from using the Internet and computers; on the contrary, it is necessary to offer such applications that may enrich the child – for example, games that support social skills or develop intelligence.

In digital parenting, the greatest emphasis is placed on the parent thoroughly explaining to the child how to safely and positively use modern technologies. To change this situation, it is necessary to actively work with children, to devote time to them, to allow them to gain experience and to increase the level of their social skills. Mainly the parents themselves are the fundamental link in this change. The parent also becomes the primary intermediary through whom the child learns about the world. At an early age, a child may be taught basic principles they will use later in life – for example, verifying information, being careful about what information to reveal about oneself to others, how to behave in a safe way on the Internet, and what risks involved on the Internet one may encounter. Just as a parent teaches a child that they shall not, for example, cross the road when there is a red light, the principles of safe use of IT technologies should be instilled in the child from an early age, as well as follow the principles intended for the parents themselves: for example, to activate the parental filter on the child's computer and filter out inappropriate content (e.g. pornographic websites), protect the computer with an antivirus, place the PC in a publicly accessible place in the home (and only later move it to the children's room), explore the virtual world together with the child, set rules for the child's use of the computer/laptop or tablet (e.g. length, frequency, purpose of use), set the child's privacy on social networks while ensuring that their profile is a non-public and unknown one to avoid suspicious people writing to them.

These rules change with the increasing age of the child; for example, from around 9–10 years of age, children start actively using social networks, start sharing their own materials – photos, videos, communications with other users – and gradually become interested in human sexuality. It is therefore necessary to adapt the rules to the current situation – the child will gradually demand their privacy, demand that they have a computer in their room, and so on. During this period, children distance themselves from their parents, and it is therefore necessary for parents to be sensitive to potential problems, such as the development of addictions, bullying, etc. Kolář⁴⁴ appeals to parents: *'Due to the seriousness of this problem and its future consequences, it is important for parents to be aware and recognize that something is wrong with the child'*. The child needs to feel supported and helped to find a solution.

Parents should install safe home computer software, especially with an antivirus programme, and a firewall and legal software purchased with a valid licence and

44 Kolář, 2001.

properly updated. They should avoid some problematic situations themselves, such as visiting dubious websites, allowing the installation of various “add-ons” offered on websites, clicking on unknown links, opening attachments/links in e-mails from an unknown person, using simple passwords, or not using passwords at all.

When parents discover that a child has discovered illegal content on the Internet, they may report it, for example, using the contact form STOP Online.⁴⁵ They may also contact the Police of the Czech Republic directly, where there is a special department dealing with internet crime. In the case of harassment by a stranger via the Internet or in the event of cyberbullying, contacting the Police of the Czech Republic is also recommended. Cyberbullying, which takes place in the school environment is the responsibility of the respective school.

If we are talking about sharenting as a phenomenon that is typical of a relationship between a parent and their minor child, the legal quality of the relationship between the child and parent changes as soon as the child acquires full legal capacity. The essence of this change lies in the fact that the child is able, not only *de facto* but also *de jure*, to make decisions about their rights and obligations and to defend themselves if others interfere with their rights.⁴⁶ Children are the subject of privacy law. Parents can deal with their privacy but are limited by the law in this possibility. The protection of the rights of the child is limited by the provision of information to the child, the expression of the child’s opinion and, last but not least, the child’s ability to apply to the court or to a social and legal protection body for children.

7. Mobile Phones in Schools

In the Czech environment, the question of how to regulate the use of mobile phones by children in the school environment has resonated very strongly in recent years. For example, there is the question of whether to ban mobile phones during classes and during breaks, or whether to limit the ban only to classes, but not to breaks.

The above-mentioned research⁴⁷ showed that the majority of children (53.3%, 14,486 children) are allowed to use mobile phones at school during breaks and prohibited from using them during classes. However, they may also be allowed to use the mobile phone in classes upon the instruction of the teacher – in cases when the mobile phone becomes a didactic teaching aid/tool. However, a large number of children (41.20%, 11,198 children) are prohibited from using mobile phones at school even during breaks.

The amendment to the Education Act⁴⁸ No. 284/2020 Coll., effective from 1 October 2020, inserted a new paragraph 3 into Section 30, which explicitly states that ‘School

45 Stop online, n.d.

46 Sehnálek, 2023.

47 Kopecký and Sztokowski, 2019.

48 Act No. 561/2004 Coll., on pre-school, primary, secondary, higher vocational and other education (Education Act), as amended.

rules or internal regulations may restrict or prohibit the use of mobile phones or other electronic devices by children, pupils or students, except for their use to the extent necessary for medical reasons'. Therefore, the Headteacher can currently also prohibit the use of mobile phones or other electronic devices altogether (including during breaks, free periods, etc.). If a pupil breaks the school rules by using a mobile phone during a lesson, the teacher has the right to confiscate the mobile phone for the remainder of the lesson, if this is so defined in the school rules. However, at the end of the lesson or school day (if the teacher assesses that the pupil will continue to use the phone despite the prohibition), the teacher must return the phone to the pupil and must not ask for it to be unlocked because that would interfere with the pupil's privacy. This will prevent the teacher from further disturbing the lesson, or from further cheating or inappropriately invading the privacy of others (e.g. by filming them). The removal of mobile phones must be reasonable and proportionate and should always be supported by the school rules.⁴⁹ Therefore, if a school imposes a blanket ban on the use of mobile phones or similar devices in its school rules, including during breaks, and free periods, it is complying with the Education Act. Specific cases, such as serious, repeated cyberbullying, which cannot be prevented in any other way, may also be grounds for a blanket ban on the use of mobile devices, because, according to the provisions of Article 30(1)(c) of the Education Act, conditions for the safety and health protection of children, pupils, or students and their protection from socially pathological phenomena and from acts of discrimination, hostility, or violence can be ensured by means of school rules.

There are some statements circulating on the Internet⁵⁰ that a teacher is not entitled to confiscate a student's items. The rules for the use of personal effects may be regulated by the school rules in accordance with Article 30(1)(a) of the Education Act. According to that provision, the school rules shall regulate the details of the exercise of children, pupils and students' rights and obligations and their legal representatives in the school or educational establishment and the details of the rules of mutual relations with the staff in the school or educational establishment. The issue of the use and regulation of mobile telephones in the classroom should not be viewed solely through the lens of ownership of the object, but from the perspective of pedagogical and educational action in school establishments. In principle, regulation at school level should have an educational dimension and, therefore, even when considering the regulation of mobile phone use in a particular school, there should be a discussion of when such regulation is positive and still has an educational dimension, and when it is just a one-sided ban without respect for the context of the role that mobile phones play in the lives of young people. Often, they no longer even pay for their snacks without a phone. Concurrently, it is useful to explain to students why the regulations occur and why they are necessary and appropriate. Equally, it is very important to

49 To avoid liability for damage to the phone, the best solution is to remove the phone from the student and place it on the teacher's desk.

50 Štěpán, 2024.

discuss the issue of correct use of mobile phones in different social situations and places, as well as the issues of working safely with mobile devices and moving safely online. The attitude and approach of pupils' legal representatives is also important.

The restriction on the use of mobile phones during class corresponds with the pupil's right to education under Article 21(1)(a) of the Education Act, which presupposes that he or she will not be disturbed during class, and with the obligation of pupils to receive a proper education, in accordance with Article 22(1)(a) of the Education Act. Another reason may be the desire to ensure the legally guaranteed right of other pupils or school employees to protection of their personality or privacy pursuant to Article 81(2) of Act No. 89/2012 Coll., Civil Code, as amended. Of course, even if the use of mobile phones during breaks and free periods is allowed, the right to privacy of others (pupils and school staff) must not be violated (e.g. by pupils filming or photographing someone on their mobile phone without their consent during a break or free period when they can use their mobile phone). However, it should be stressed that the school cannot ban phones that are switched off in the bag; only their use can be banned.

8. Public Administration in the Area

State intervention is also important in the prevention of internet crime targeting children. In the Czech Republic, the prevention of risky behaviour is coordinated in parallel by several ministries – for example, the Ministry of Education, Youth and Sports focuses on so-called school prevention, the Ministry of the Interior on so-called crime prevention, the Ministry of Health on so-called health prevention, and so on. Individual prevention systems are implemented in parallel, and although they focus on similar topics, mutual communication and coordination of individual activities often fail in practice. Additionally, prevention is also dealt with by supra-departmental bodies, such as the Government Council for Coordination of Anti-Drug Policy at the Government Office and the Republic Committee for Crime Prevention at the Ministry of the Interior – all relevant departments are then represented in these bodies. Cooperation, unification of approaches and coordination of activities in the given area across departments is the goal of the working groups. The Ministry of Education, Youth and Sports also methodically leads and coordinates the network of school coordinators, which is made up of regional school coordinators of prevention, prevention methodologies, and school prevention methodologies. In particular, school prevention methodology is the key actor in the prevention of risky behaviour at the school level. The school prevention methodologist performs methodological, coordination, information, and advisory activities; their work mainly includes the preparation and implementation of preventive programmes for the given school and school facilities that are part of the school education programme.

The National Cyber and Information Security Agency (NÚKIB), whose executive element is the National Cyber Security Center (NCKB), is the manager of cyber security.

9. Conclusion

Children cannot be banned from the Internet. It is the responsibility of adults, both parents and especially schools to teach them how to navigate digital space, to know its risks, and to seek help if necessary. The Internet is attractive to children mainly because it brings them entertainment. They listen to music, watch films, or communicate with friends on social networks, mainly on Facebook or Instagram. The vast majority of them also use the Internet to prepare for school. Even the youngest children, specifically a third of children between the ages of 9 and 10, have fun with friends and acquaintances through social networks. From the age of 13, it is almost a matter of course to be a member of one of the social networks. Almost 80% of children between the ages of 13 and 14 and almost 90% of children between the ages of 15 and 16 are on Facebook.

Many non-profit organisations in the Czech Republic deal with the protection of children on the Internet, such as AVAST, which teaches children how to behave on the Internet with its Be safe online project⁵¹; it is also used by the Ministry of Education as a recommendation subject matter for schools. Furthermore, this protection is ensured by the organisations named E-bezpečí (E-safety),⁵² Linka bezpečí (Helpline),⁵³ and the Safer Internet Centre.⁵⁴

The main objective of the study was to determine the legislative limits of the definition and fulfilment of the concept of digital behaviour of the child. In my opinion, the primary responsibility for protecting the rights of the child in cyberspace lies with the parents, related to the exercise of their parental responsibility. The legal limits of determining the best interests of the child are given; it is up to adults how they will protect them.

51 See: <https://www.avast.com/cz/besafeonline/> (Accessed: 3 August 2025).

52 See: <https://www.e-bezpeci.cz/index.php/component/tags/tag/poradenstvi> (Accessed: 3 August 2025).

53 See: https://www.linkabezpeci.cz/?gclid=EAIaIQobChMIm_SDtYD9gQMVy-Z3Ch1zRgxNEAA YASABEgJslvD_BwE (Accessed: 3 August 2025).

54 See: <https://www.bezpecnyinternet.cz/cs/> (Accessed: 3 August 2025).

Bibliography

- Citterbergerová, A. (2023) 'Protecting children's right to privacy in the social media sphere: sharenting in the European law perspective', *Jurisprudence*, 2023/3, pp. 22–32.
- Černá, A. (2013) *Cyberbullying: a guide to a new phenomenon*. 1st edn. Praha: Grada.
- Dixon, S.J. (last update 2025) Most popular social media networks worldwide as of February 2025, by number of monthly active users, *statista*, 26 March [Online]. Available at: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (Accessed: 1 October 2023).
- Hofschneiderová, A. (2017) 'O konceptu nejlepšího zájmu dítěte', *epravo.cz*, 17 October [Online]. Available at: <https://www.epravo.cz/top/clanky/o-konceptu-nejlepsiho-zajmu-dite-106509.html> (Accessed: 3 August 2025).
- Keith, S., Martin, M.E. (2005) 'Cyber- bullying: Creating a culture of respect in a cyber world', *Reclaiming children and Youth*, 13(4), pp. 224–228.
- Kolář, M. (2001) *Bolest šikanování*. 1st edn. Praha: Portal.
- Kopecký, K., Sztokowski, R. (2019) *České děti v kybersvětě*. Olomouci: Univerzita Palackého v Olomouci [Online]. Available at: <https://o2chytraskola.cz/vyzkumy/ceske-deti-v-kybersvete> (Accessed: 3 August 2025).
- Livingstone, M., Haddon L (2011) 'EuKids Online: Final Report', *Zeitschrift fur psychologie – Journal of psychology*, 217(4), pp. 236–239; <https://doi.org/10.1027/0044-3409.217.4.233>.
- Sehnálek, D. (2023) 'Sharenting and children's privacy protection in International, EU, and Czech law: Parents, stop sharing! Thank you, your children', *Central European Journal of Comparative Law*, 4(1), pp. 111–132; <https://doi.org/10.47078/2023.1.111-132>.
- Štěpán, R. (2024) 'Mobil jako soukromý majetek: Učitel ho žákovi dlouhodobě zabavit nesmí a pravidla se dají ohýbat', *Epenize*, 26 January [Online]. Available at: <https://www.epenize.eu/mobil-jako-soukromy-majetek-ucitel-ho-zakovi-dlouhodobě-zabavit-nesmi-a-pravidla-se-daji-ohybat/2> (a teacher may not confiscate a mobile phone as private property in the long term) (Accessed: 3 August 2025).
- Stop online (n.d.) 'Ohlaste nezákonný obsah', *stoponline.cz* [Online]. Available at: <https://www.stoponline.cz/cs/> (Accessed: 3 August 2025).
- UNICEF (2018) *Children's online privacy and freedom of expression*. New York: UNICEF [Online]. Available at: <https://www.unicef.org/childrightsandbusiness/media/291/file/UNICEF-Childrens-Online-Privacy-and-Freedom-of-Expression.pdf> (Accessed: 3 August 2025).
- Více našich webů (2009) 'Kybersíkana a její prevence' [Online]. Available at: <https://www.clovekvtisni.cz/kybersikana-a-její-prevention-103pub> (Accessed: 23 January 2021).

Children in Digital Age – Hungarian Perspective

Csenge HALÁSZ

ABSTRACT

This chapter explores the legal framework for protecting children's rights in Hungary, with particular emphasis on the challenges posed by internet and social media use. It begins by outlining the Hungarian legal definitions of childhood and minority, demonstrating how these relate to capacity, education, and criminal responsibility. The analysis highlights the growing presence of children on digital platforms and examines the potential threats to their fundamental rights, including privacy, freedom of expression, and protection from harmful content. Particular attention is paid to inconsistencies between international platform policies (e.g., Facebook's age requirements) and Hungarian civil law. The chapter also investigates the phenomenon of "sharenting" and its impact on children's privacy and identity development. It addresses legal gaps regarding parental overexposure of children online and the lack of sector-specific regulation. Case law in this field remains limited, but empirical studies indicate widespread online harm among minors. Institutional mechanisms—such as the National Media and Infocommunications Authority and NGOs like the Hintalovon Foundation—play an active role in education and prevention. In conclusion, while Hungary's legal system provides a comprehensive basis for child protection, the rapid evolution of digital environments necessitates further regulatory adaptation and awareness-raising initiatives.

KEYWORDS

personality rights, children's rights, social media, right to privacy, fundamental rights

1. Definitions and Taxonomic Rationale

The starting point for the research on the Hungarian legal system is a conceptual and taxonomic framework, which includes an overview of the most important definitions and legal bases, as well as the latest available statistical data on children's Internet use.¹

In the Hungarian legal system – as in most of the legal systems examined in this textbook – the concept of the child is based on the United Nations Convention on the Rights of the Child (CRC). The document is also part of the Hungarian legal system, as

1 CRC, adopted in New York on 20 November 1989.

Csenge HALÁSZ (2025) 'Children in Digital Age – Hungarian Perspective' in Halász, Cs. (ed.) *Children in Digital Age*. Miskolc–Budapest: Central European Academic Publishing, pp. 153–169.
https://doi.org/10.71009/2025.csh.cida_8.

it was ratified by Act LXIV of 1991.² According to this Convention, ‘a child is a person who has not attained the age of eighteen years, unless he or she has attained the age of majority earlier under the law applicable to him or her’.³ Domestic legislation, therefore, considers the age of 18 to mark the end of childhood, although some laws may impose different age limits.

The Hungarian Civil Code uses the term “minor”. It states that a minor is someone who has not reached the age of eighteen, but that a minor can become an adult by marriage.⁴ The marriage of a minor may take place after the age of 16 with the permission of the guardianship authorities. Current civil law imposes significant legal consequences for reaching the age of 14. The legislator applies an irrebuttable presumption that a minor under the age of 14 is incompetent.⁵ However, the Civil Code, *expressis verbis*, exempts children under the age of 14 from this requirement in the case of minor transactions of everyday life, allowing their legal representative to act on their behalf.⁶ Minors between the ages of fourteen and eighteen who are not incapacitated have limited capacity.⁷ As a general rule, the consent of their legal representative is required for the validity of their legal declarations, although the Civil Code provides for exceptions in certain cases.⁸ Hungarian civil law, therefore, differentiates between legal entities of child age, according to which legal declarations made by children under the age of fourteen are invalid as a general rule, while those made by children between the ages of fourteen and eighteen are valid with the consent of their legal representative.⁹

In the area of criminal law, the Hungarian Criminal Code lists childhood as one of the grounds for exclusion or limitation of criminal liability.¹⁰ Under the Criminal Code, a person under the age of 14 is not punishable.¹¹ An exception is made for certain offences if the offender was over the age of 12 and had the necessary discernment to understand the consequences of the offence at the time of committing it.¹²

The law on national public education also differentiates between persons of child age, stating that all children are obliged to attend institutional education, i.e., compulsory schooling. As regards the starting date, the law states that a child becomes of compulsory school age in the year in which he or she reaches the age of six by

2 Act LXIV of 1991 on the proclamation of the CRC, signed in New York on 20 November 1989.

3 Part I Art. 1 of Act LXIV of 1991.

4 Art. 2:10 of Act V of 2013 on the Civil Code (“Civil Code”).

5 Art. 2:13 of Civil Code.

6 Ibid., Art. 2:14 paras. 1–2.

7 Ibid., Art. 2:11.

8 See also: Ibid., Art. 2:12 para. 2.

9 Act C of 2012 on the Criminal Code (“Criminal Code”).

10 Art. 15 of Criminal Code.

11 According to Art. 16 of the Criminal Code, such offences include manslaughter, murder committed with violence, assault, violence against public officials and persons performing official duties, terrorist offences, robbery, and pillage.

12 Act CXC of 2011 on National Public Education (“Public Education Act”).

31 August.¹³ The obligation lasts until the end of the school year in which the child reaches the age of 16.¹⁴

An interesting regulatory methodology is followed by the law on the basic rules and certain restrictions on commercial advertising, which in its general provisions distinguishes between children and minors.¹⁵ According to the provisions of this law, a person who has not yet reached the age of 14 is considered to be a minor, while a juvenile is a person who has reached the age of 14 but not yet 18. Based on these examples, the concept of “children” can be considered uniform in Hungarian law, in line with the CRC. However, individual sectoral rules differentiate between persons of child age with regard to their level of maturity and capacity for discernment.

The protection of children’s rights and the primacy of their interests are ensured by a number of laws in the Hungarian legal system. Among these, Act LXIV of 1991 transposing the CRC into the domestic legal system has already been highlighted at the beginning of this chapter. In addition, the basis of the legislation is, of course, created by the Fundamental Law, which declares in Art. XVI that every child has the right to the protection and care necessary for healthy physical, mental, and moral development.¹⁶ This is the basis of both the Civil Code and the Family Code, which include the protection of the best interests of the child as a fundamental principle, as reflected in the relevant family law provisions.¹⁷ In relation to our topic, the section of the Civil Code dealing with the rights of the person is also worth highlighting, given that the rights of the person are the rights of all people, including children.

The Civil Code lays down a general rule for the protection of personality, then highlights certain specific rights, and finally sets out the system of sanctions for the protection of personality.¹⁸ Regarding the enforcement of personality rights, the Civil Code states that any person may enforce them personally. A minor with limited capacity to act may defend his or her rights as a person in his or her own right, while a minor who is incapacitated may be defended by his or her legal representative.¹⁹ An integral part of the national legislation on child protection is the Act on the Administration of Guardianship, which declares the rights of the child, sets out rules on childcare, and establishes the institutional system of child protection.²⁰ Without being exhaustive, in addition to the above-mentioned legislation, there are also provisions affecting children’s rights in other legislation, such as the Act on Economic Advertising, the

13 Art. 45 para. 2 of Public Education Act.

14 Ibid., Art. 45 para. 3.

15 Art. 2 points c) and e) of Act XLVIII of 2008 on the basic conditions and certain restrictions on commercial advertising (“Advertising Act”).

16 Art. XVI para. 1 of the Fundamental Law.

17 Art. 4:2 of Civil Code.

18 Arts. 2:42–2:54 of Civil Code.

19 Ibid., Art. 2:54 para. 2.

20 See for example: Chapter II, Chapter IV, Chapter V, Chapter V, Chapter V of Act XXXI of 1997 on the protection of children and the administration of guardianship (in brief: Gyvtv.)

Government Decree on Home Renovation Assistance for Children, and the Government Decree on Guardianship Authorities.²¹

The Hungarian legislation on the legal status and rights of children is both comprehensive and provides adequate legal protection for the age group concerned. However, one of the most important questions concerning our topic is: to what extent does the existing regulatory environment protect the rights of children using the Internet?

The issue is extremely topical in 2023, as confirmed by the statistics of the National Media and Infocommunications Authority (NMHH). According to a report published in 2022, 97.1% of the 15–50 age group use the Internet, and addiction starts at a very young age. Data from families surveyed show that 4% of two-year-old children and 9% of three-year-olds use the Internet.²² People under 18 are the most frequent users of social networking sites, with 65% of Internet users in the European Union spending more than half an hour a day on a social networking site. Facebook is considered the leader in the country (in line with global statistics), but the most popular social networking sites for 16–25-year-olds are Instagram, TikTok, and YouTube.²³ The use of these platforms can be considered highly addictive, with colourful and constantly changing content “spinning” as part of children’s daily routine. In practice, they spend a very large part of their social lives on these platforms, using the Internet to find information, share content, and receive targeted advertising – but, unfortunately, also with the risk of becoming both perpetrators and victims of infringements.

In the rest of the chapter, we will examine how the protection of the rights of children using the Internet is developing in the Hungarian legal system, which institutions help to protect the rights, and what case law decisions have been made. After drawing forward-looking conclusions, we will also make some regulatory proposals.

2. Children’s Rights on Internet Platforms

According to relevant statistics from the National Media and Communications Authority, the proportion of children using smartphones exceeds 85%, and at least three-quarters of children aged between 9 and 16 have a profile on a social media site.²⁴ Children can access virtually any online platform with a few clicks. On the one hand, this has positive consequences, as online platforms can facilitate access to information, enable interaction, and, where appropriate, broaden horizons and provide educational content. However, online platforms can also have negative effects on children’s rights. Research by the NMHH also found that almost a quarter of Hungarian children have come into contact with someone they did not know online, and

21 Government Decree 149/1997 (IX. 10.) on Guardianship Authorities and Child Protection and Guardianship Procedures.

22 NMHH, 2022a.

23 NMHH, 2023, p. 29.

24 NMHH, n.d.a

nearly a third have met someone they did not know in person.²⁵ In view of this, and in order to eliminate situations that put children at risk online, from 1 July 2014, Internet access providers have been obliged to make some form of child protection filtering software available on their websites for download and use.²⁶

Turning to the legal environment, it is first worth clarifying which of the specific rights of children are the most commonly infringed when using certain Internet platforms. In this respect, both children's rights and children's rights as individuals will be examined. The scope of children's rights is also declared in the CRC. For children who use social media, the implementation of these rights is examined in two sets of relationships: the first is the relationship between social networking sites and child users, while the second is the relationship between users themselves.²⁷

2.1. Children's Rights in the Relationship Between the Social Networking Site and the User

For an individual to become a user of a social networking site, they merely need to provide their personal data, accept the platform's general terms and conditions, and click on the registration button. However, the accuracy of the data provided is not verified.²⁸ This creates a risk that children who would otherwise not be able to register on a social networking site under the current legislation may do so.

Regarding the age limit for registration, the Facebook Terms of Use and the Hungarian Civil Code contain different rules. According to Facebook's Terms of Use, no person under the age of 13 may be a user of the platform.²⁹ As the detection of false data during registration is not guaranteed, Facebook provides an online platform called "Report a Minor User", which allows any user to report any profile believed to be operated by a person under the age of 13.³⁰

By contrast, as explained in the first part of this chapter, the Civil Code links the onset of legal capacity to the age of 14 and attaches the legal consequence of nullity to the independent declaration of legal capacity by an incapacitated minor. The legal relationship between the user and the social networking site can clearly be regarded as a contractual legal relationship, meaning that, under national legislation, a minor under the age of 14 is not entitled to make such a contractual declaration independently, without a legal representative.³¹ Thus, there is a contradiction between the

²⁵ Ibid.

²⁶ Ibid.

²⁷ On this issue, see the study below: Barzó and Fráter-Bihari, 2025.

²⁸ Note that the contract between the community portal provider and you is established during the registration process. The contract is concluded between absentees and can be considered as a consumer contract and a contract concluded under general terms and conditions between absentees.

²⁹ Legal terms of Facebook [Online]. Available at: <https://www.facebook.com/legal/terms/update.4.5> (Accessed: 12 August 2023).

³⁰ Facebook Help Center [Online]. Available at: <https://www.facebook.com/help/contact/209046679279097> (Accessed: 28 August 2023).

³¹ Art. 2:14 para. 1 of Civil Code.

general terms and conditions of Facebook and domestic legislation with regard to minors aged between 13 and 14. According to the Terms of Use, it is possible to register on the site at the age of 13, whereas, under the logic explained above, this is not possible under domestic law. The Hungarian Civil Code does not consider the declaration of a minor to be null and void if the contract concluded and performed by him/her is of minor importance, and the conclusion of which is a common occurrence in everyday life and does not require any special consideration.³² However, it is questionable whether the exception laid down by law can be applied in the case of Facebook registration of a minor. The act is undoubtedly a mass transaction in everyday life, but is it of minor importance? The answer will be developed in future case law; in our view, it is not possible to include the use of a social networking site in this scope with any certainty, given the dangers mentioned and described above.

In this context, the limited capacity of persons aged between 14 and 18 should also be mentioned, since, in view of their age, it is often persons in this age group who engage in infringements of their personality rights on social networking sites, and whose personality rights are also frequently infringed upon via these platforms. Here too, it is important to emphasise that the parents or guardians of minors have a special role to play in informing them of the rules of use and drawing their attention to potential dangers.³³

Once registered, the minor becomes a user of the social networking site, which essentially means he or she becomes part of the online community of that platform. In the following, we will examine the rights of children on these platforms, in relation to the functioning of social networking sites, which raises legislative and enforcement issues.

First among these is the right of children to express their views. Freedom of expression is a fundamental right declared in Art. IX of the Fundamental Law, which is a right of every human being. It can be considered a communication mother right, applying not only to oral and written communications but also to online communications.³⁴ This right extends to the right to information, under the protection of freedom of expression, but it is not unlimited.³⁵ Freedom of expression has traditionally been limited by child protection provisions. These norms are also regulated in the Hungarian Advertising Act, which states that advertising that may harm the physical, mental,

32 Ibid., Art. 2:14 para. 2.

33 For the sake of completeness, what happens when someone's privacy is violated by a minor user on Facebook? In this case, the concept of fault, otherwise used in tort law, could be a starting point. This could potentially make the Civil Code applicable. "Liability for damage caused to a person who is not at fault". In our opinion, future case law will have to interpret these rules in a specific way, since it is questionable to what extent a body of rules which essentially establishes the liability of the carer for the damage caused by the incapable person will fulfil its purpose.

34 Koltay, 2018.

35 Art. IX paras. 2–6 of the Fundamental Law.

moral, or emotional development of children and minors is prohibited.³⁶ At the outset, these requirements must also apply to social networking sites. Children using these platforms naturally have the same right to freedom of expression as adult users. This fundamental right of children is also confirmed in Art. 13 of the CRC and in Art. 8 of the Children's Act. Children exercise their communication rights on a very wide range of social media platforms, as they create virtually untraceable amounts of text entries and share photos, videos, and audio recordings on a global scale, conducting a significant part of their personal communication via these online platforms. However, the exercise of these rights by users under the age of majority must be accompanied by respect for the rights of others. A significant percentage of young users are unaware of the situations in which their online communications fall within the scope of freedom of expression and those likely to constitute an infringement. The right to information, which is also covered by the right to freedom of expression, is significantly affected by the rise of social media. This can be traced back to the statistics outlined above, according to which more than 97% of Internet users in Hungary, including children, spend at least half an hour a day browsing a social networking site. This means that a significant proportion of people use these platforms to find information. Social media also pose a risk of information leakage through the spread of fake news and the display of completely personalised content. The dissemination of disinformation on social networking sites means that it is also accessible to a wide range of child users. The Digital Services Act Regulation and the European Union have a strong objective to reduce disinformation on social networking sites, which also positively impacts children's right to information. Social networking sites are using algorithms to stop the spread of fake news, for which the European Union published a practical guide in 2022. The customisation of content used by social networking sites seems to be a very "convenient" setting, but it also risks limiting the individual user to the content defined by the algorithms, thus preventing them from encountering different preferences, content, and news. For child users, it is important to ensure that they are exposed to educational content appropriate to their interests and age, which could also help their development.

The algorithms used by social networking sites also have a significant impact on the privacy rights of individual users.³⁷ The protection of privacy is a fundamental right declared in the Fundamental Law, the right to privacy in the Civil Code, and provided for by Act LIII of 2018 as a separate piece of legislation.³⁸ The Privacy Protection Act already notes in its preamble that modern means of infocommunication have changed the norms of daily interaction, so the protection of the right to privacy extends to both physical and online harassment.³⁹ Children's right to privacy is also

36 Art. 8 of Advertising Act. In this section, the legislator also states that it is prohibited to make available to persons under 18 years of age advertisements that depict sexuality for its own sake or that depict a minor in a dangerous or sexual situation.

37 Art. VI para. 1 of the Fundamental Law.

38 Act LIII of 2018 on the Protection of Privacy (hereinafter: Privacy Protection Act).

39 Mvtv. Preambulum.

declared in the CRC under Art. 16. The legal framework is in place, but the so-called “zero-price” business model of social networking sites has a major impact on children’s right to privacy. At the heart of this model is the fact that the content shared and frequently updated on social platforms attracts a constant flow of consumers, whose activity is collected by the platform provider through the various methods outlined above.⁴⁰ With this information, social networking sites provide targeted advertising opportunities to their business clients. These clients, in turn, target their advertisements to users – who, based on the profile extracted from the personal data, can be considered as potential customers or users of the services they offer – on the users’ News Feed. Social networking sites keep the workings of their algorithms a trade secret, but it is certain that they monitor users’ preferences in detail to compile the content of their personal News Feed.⁴¹ To this end, social networking sites’ AI-powered algorithms monitor with whom frequent users of the platform’s chat service communicate, as well as which posts they like, share, or comment on. As a consequence of monitoring all these activities, the algorithm displays the content of the users with whom they interact closely in the online space.⁴² The same is true for the advertisements on the Message Board: the advertisements that users view for a longer period of time, or respond to in some way, will be seen more often on the Timeline (along with similar advertisements).

The creation of these targeted advertisements, the monitoring of users, the collection of their data, and the identification of their personal preferences clearly affect children using social networking sites. One need only think here of the TikTok app, which is used predominantly by this age group and whose data management practices give rise to numerous concerns. The operator of the platform constantly collects personal data and analyses the preferences of underage users, which allows users as young as 14 to be constantly exposed to personalised advertising. In our view, this practice is extremely worrying from the perspective of protecting the privacy rights of underage users, particularly their right to privacy, since this advertising method effectively commodifies the privacy of minors. It is also a problematic practice that, while the media law of some states, for example, imposes strict conditions on linear media providers regarding advertising to minors, the practice of social networking sites, as described above, is essentially free to continue.⁴³ Among other things, this is the aim of the Digital Services Act Regulation adopted under the auspices of the European Union, which, based on the results of impact assessments, has also set out in its explanatory memorandum the need for greater protection of the fundamental rights and privacy of users, particularly with regard to vulnerable groups such as minors.

40 Pásztélyi and Bordács, 2020, pp. 25–32.

41 Auer and Joó, 2019, p. 6.

42 Ibid.

43 Digital Services Act Regulation. Rationale. Results of ex post evaluations, stakeholder consultations and impact assessments. Fundamental rights.

In addition to the protection of freedom of expression and the right to privacy, Internet sites to which minors have access must also comply with the requirement in the CRC that they must not impair the mental and moral development of minors.⁴⁴ The enforcement and enforceability of this requirement pose a number of technical and legal challenges, but the protection of minors from harmful content on the Internet, which is very characteristic of social media platforms, is of social interest.

2.2. Children's Rights in the Legal Relationship Between Users

We have just outlined the rights that children have in their relationship with the portal. However, the rights of children using certain Internet platforms can also be violated by the behaviour of individual users. Trends in Hungarian judicial practice show that violations of individual personality rights frequently occur on social networking sites. Comments that are defamatory or damaging to reputation, the misuse of personal data, violations of privacy, and the unauthorised publication of images or audio recordings have become practically commonplace on certain online platforms. Children using social networking sites may be particularly vulnerable to these infringements, as they are often unaware of the unlawful nature of their conduct due to their age. For example, the photos they send and the content they post in “closed” chat groups may constitute an offence against their right to privacy.

In addition to conduct that violates children's privacy rights, humiliating messages and comments posted on social networking sites, unauthorised posting of images of the victim in embarrassing or vulnerable situations, and messages with sexual content can also lead to criminal prosecution. The Hungarian legislator has criminalised harassment in the Criminal Code, which increasingly uses the online space as a “place of offence”.⁴⁵ Such behaviour is referred to in the literature as cyberbullying and constitutes a specific group of online harms to children.⁴⁶ According to a study published in 2020 in Hungary, nearly 69% of primary school-age children and 73% of secondary school-age children have experienced online bullying.

Online bullying causes serious psychological, emotional, and social harm. Electronic communication emboldens perpetrators because they cannot see the emotional reactions of their victims, making it easier to commit the act without feeling guilty. Thus, in many cases, they do not realise the negative impact of their actions on the victim, as they may think they are simply participating in a relatively harmless “prank”. However, online harassment can have serious consequences for victims, such as loss of self-confidence, depression, later use of mind-altering drugs, or aggression. In extreme cases, persistent depression can even lead to suicide in the absence of appropriate support. Becoming a victim of online bullying can also lead to later deviance, including criminality, as the victim may themselves become an abuser. Reducing the number of children who become victims of online bullying

44 Art. 14 of the CRC.

45 Art. 222 of Criminal Code.

46 NMHH, 2022b.

is in the interest of society as a whole. One way to achieve this is by raising media awareness, involving not only children but also parents and teachers.

2.3. A Specific Issue: Impact of Sharenting on Children's Rights

In addition to the distinctions in the relational systems influencing children's rights in the online space, we must also consider parents' activities involving their children on social media. This is justified by the fact that parents often share their children's photos and personal data on social media platforms. This phenomenon is commonly referred to in research and academic articles as "sharenting", a portmanteau of "sharing" and "parent".⁴⁷ It is not possible to translate this term into English using a single word, so for the purposes of this chapter, we will use the general term "sharing" to refer to the frequent posting of photos, videos, and text about children on social media by parents (or other relatives, such as grandparents).⁴⁸ While it is difficult to make precise statements about the frequency of such sharing, regular posting within short intervals can be considered part of this category, provided that the information shared is intimate and private to the child.⁴⁹

The term "digital footprint" is also used to describe content published about children. Its importance is illustrated by a 2018 New York Post article, which estimated that by the time a child reaches the age of 13, around 1,300 posts about them will have been published online.⁵⁰ Recent research has also shown that 74% of social media users know parents who over-share photos and other personal information about their children on various social media platforms.⁵¹

In Hungary, the publication of photographs and records of children is a very common practice among parents. According to Art. 2:54 (2) of the Civil Code, the legal representative may take action to protect the personal rights of children who are incapacitated. Under this provision, the legal representative of the child (usually the parent) has the right to decide on the publication of photographs and communications about their child and to act in the child's best interests regarding media content published by others. However, parents cannot exercise this right without limitation. Art. XVI (1) of the Fundamental Law declares that every child has the right to such protection and care as is necessary for his or her proper physical, mental, and moral development. It follows from this provision that parents may only publish photographs and videos of their children if these do not endanger the child's physical, mental, or moral development. Therefore, when parents share content about their children on social media, they should exercise caution and consider the best interests of the child, refraining from posting any material that could jeopardise the child's healthy development. In our view, photographs or videos showing a child in a vulnerable situation, such as in inadequate clothing or a ridiculous scenario, can adversely affect

47 See for example: Verswijvel, et al., 2019; Gál, 2020, pp. 19–25.

48 For more on this see: Steinberg, 2017, pp. 16–41.

49 See for more in: Azucar, Marengo and Settanni, 2017.

50 Dellato, 2018.

51 Vinney, 2022.

the child's psychological development. This also includes posts containing intimate information about the child, as they may negatively impact the child's mental health in later life, in addition to clearly violating their privacy.⁵² Extensive sociological and psychological research is currently being conducted into the impact of parents' excessive presence on social media on their children's later psychological development. Some studies suggest that parents' oversharing of information about their children, combined with feedback from their social circles, may also have a negative impact on children's identity development.⁵³

The protection of children's rights is reinforced by Art. 8 of the Children's Act, which declares that children have the right to express their views, to be informed of their rights, and to be heard in all matters concerning them.⁵⁴ A similar right is enshrined in the 1989 New York Convention, Art. 12 of which states that the views of the child shall be considered in accordance with his or her age and maturity in all matters affecting him or her. Under these provisions, the consent of a child who is capable of expressing his or her views must be obtained by the parent before publishing photographs or communications about the child. Clearly, an infant or a very young child is not capable of such expression, making "baby photos" on social networking sites a controversial issue.

Two opposing views prevail in public opinion on this issue. One view is that children who are not yet capable of expressing their views should not be photographed or have private communications shared for the reasons outlined above.⁵⁵ The other view is that such a requirement would be excessive in today's world, given the pervasive nature of social media in people's lives, and that it would be unrealistic to expect parents not to share any content about the joys of raising children and their development.

In our view, the aforementioned legal requirements to refrain from publishing images of children in a vulnerable position should also apply to baby photos.⁵⁶ The publication of photos and videos of children in such situations is not justified and does not strike a balance between the interests of the parents as "private individuals" and the advertising activities of parents who may act as online opinion leaders (influencers). In light of this, it would be justified to restrict the advertising activities of opinion leaders in this area, although there is currently no legislative intent at the national level to do so.⁵⁷

Regarding the phenomenon of sharenting, violations of minors' privacy rights on social media frequently take the form of photos, videos, and text posts shared by parents. This often includes the exposure of private footage of children to thousands

52 For more see: Ranzini, Newlands and Lutz, 2020, pp. 1–13.

53 Vinney, 2022.

54 Art. 8 para. 1 of Act XXXI of 1997 on the Protection of Children and the Administration of Guardianship.

55 See also: Hintalovon Gyermekjogi Alapítvány, n.d.a.

56 Gazdasági Versenyhivatal, 2022.

57 See also: Archer, 2019; Jorge et al., 2022, p. 166.

of followers of a parent acting as an opinion leader to promote a product or service. In Hungary, Chapter I of the Media Services and Mass Communications Act also contains provisions on the protection of minors, and the Advertising Act reflects this protection for those under 14. However, these rules are rather general in nature. Consequently, it is essential to establish specific rules for social media in the future, which would balance the vulnerable position of minors on online platforms and facilitate the effective exercise of their rights as individuals.

3. Presentation of the Case Law in the Area Concerned

In Hungary, there is currently no known case law that specifically addresses the violation of children's rights in the online space. According to the Psyma research published by the NMHH in 2021, a significant percentage of Hungarian children using the Internet have experienced online bullying.⁵⁸ For example, in 2020, 36% of 15- and 16-year-old users experienced some form of online bullying.⁵⁹

In our view, a considerable amount of online conduct that violates children's rights does not reach the courts because, in many cases, neither the offender nor the victim realises that the conduct in question constitutes a violation of privacy rights. Even within school communities and groups of friends – key areas of children's social activity – there are incidents in which a photograph of a minor is posted on social media without his or her consent, often in an embarrassing situation, and various derogatory or disparaging comments are common in the online activities of this age group.

Raising media awareness plays a key role in discouraging such activities, and the institutions described in the next sub-chapter have a crucial part to play in this effort.

4. Institutions to Protect Children's Rights Online

The Hungarian child protection system is extensive and well-developed. At the regional level, Child Protection Centres and Regional Child Protection Specialist Services provide comprehensive child protection services.⁶⁰

Since 2022, the sectoral management of child protection has been the responsibility of the Ministry of the Interior, as well as the Ministry of Culture and Innovation, under which the Secretary of State for Families operates.⁶¹

⁵⁸ NMHH, 2021, p. 142.

⁵⁹ Ibid.

⁶⁰ Országos Gyermekvédelmi Szakszolgálat, n.d.

⁶¹ Ibid.

Regarding the protection of children's rights online, the activities of the NMHH are particularly noteworthy. One of its priority programmes is the promotion of the protection of minors' rights in the online space. To this end, the Internet Round Table for the Protection of Children was launched on 1 March 2014.⁶² The Round Table, composed of 21 members, develops recommendations and positions to support the work of the President of the NMHH. Its aim is to produce documents that promote child-friendly Internet use and encourage the conscious use of the Internet by children and their parents. In addition to public authority representatives, the 21-member body includes representatives of non-governmental organisations and media professionals.⁶³

The launch of the Bűvösvölgy Media Literacy Training Centre ("Centre") is also an NMHH initiative aimed at raising media awareness.⁶⁴ The Centre offers a wide range of programmes for school groups from across Hungary, free of charge. It welcomes groups of children aged 9–16 years in three locations: Budapest, Debrecen, and Sopron. Sessions last approximately 5–6 hours and are designed to enhance media literacy through interactive group activities. One session, "Net Risk", introduces participants to online privacy, harassment, and cyberbullying in a situational game and raises awareness of the potential legal consequences.⁶⁵ Another session, "Netchecker", introduces children to useful websites and applications.

The NMHH's media awareness activities also include numerous educational materials available on its website, providing excellent resources for children, parents, and teachers alike.⁶⁶

Regarding the protection of children's rights at the state level, the Digital Well-being Programme 2.0⁶⁷ was launched in 2017 as a government initiative, aiming to improve Internet use and digital awareness among the population. Although the programme ended on 31 March 2023, Hungary's Digital Child Protection Strategy, adopted in 2016 under its auspices, remains in force.⁶⁸ This Government Decision essentially expresses the Government's commitment to digital child protection, to be implemented through measures such as developing filtering software and providing extensive information to the public. As noted in a previous sub-chapter, since 2014, Internet service providers in Hungary have been required to make some form of child protection filtering system available on their websites.⁶⁹

62 The legal basis was created by the 2013 amendment to Act CVIII of 2001 on certain issues of information society services.

63 NMHH, n.d.c.

64 Bűvösvölgy Médiaértés-oktató Központ (Magic Valley Media Literacy Training Centre) [Online]. Available at: <https://buvosvolgy.hu> (Accessed: 4 November 2023).

65 Ibid.

66 See, as an example, the platform Information for consumers: NMHH, n.d.b.

67 See: Government of Hungary, 2017.

68 See also: Government Decision 1488/2016 (IX.2.)

69 NMHH, n.d.a.

Additionally, the Hintalovon Children's Rights Foundation, a non-governmental organisation operating since 2015, runs several programmes.⁷⁰ Two notable initiatives are the "Child-Friendly Media and Advertising Project" and the "Digital Parent" programme. The latter focuses on raising parents' media literacy to promote responsible and exemplary behaviour and to discourage sharenting.⁷¹

5. Summary

Overall, Hungary has a broad regulatory environment protecting children's rights. The legislator adapts the concept of the child to align with the CRC, while sectoral rules differentiate between children according to their age. Children's rights on the Internet, particularly on social media platforms, face a number of challenges. In this area, we have distinguished between the legal relationship between the social networking site provider and the child as a user, and the relationship between users themselves. Regarding the former contractual relationship, the European Union's Digital Services Act Regulation sets out stricter rules for online service providers, which will also help to protect children's rights in the long term. In addition to effective legislative and enforcement responses to infringements arising from users' interactions, raising awareness of the Internet can also help. The phenomenon of sharenting is also worthy of mention in this context, and its legal regulation is a matter for the legislator to consider. In our view, the introduction of such regulation in separate legislation would be a welcome development, although the prohibition of advertising by opinion leaders to children could also be included in Art. 8 of the Advertising Act.

After examining these relationships, it can be concluded that children's rights to healthy development, expression, privacy, images and sound recordings, personal data, and honour and reputation may be violated on various online platforms. A high level of protection of these rights is therefore a priority. In this regard, alongside legislation, the institutions described in this chapter will help to ensure that digital child protection in Hungary is implemented to a high standard and keeps pace with rapid technological developments.

70 See also: Hintalovon Gyermekjogi Alapítvány, n.d.c.

71 See also: Hintalovon Gyermekjogi Alapítvány, n.d.b.

Bibliography

- Archer, C. (2019) 'How influencer 'mumpreneur' bloggers and 'everyday' mums frame presenting their children online', *Media International Australia*, 170(1), pp. 47–56; <https://doi.org/10.1177/1329878X19828365>.
- Azucar, D., Marengo, D., Settanni, M. (2017) 'Predicting the Big 5 personality traits from digital footprints on social media: a meta-analysis', *Personality and Individual Differences*, 2017/124, pp. 150–159; <https://doi.org/10.1016/j.paid.2017.12.018>.
- Auer, Á., Joó, T. (eds.) (2019) *Hálózatok a közszolgáltatásban*. Budapest: Dialóg Campus [Online]. Available at: <http://real.mtak.hu/107966/1/Lelektanimuveletekeskozsegimedia.pdf> (Accessed: 5 July 2022).
- Barzó, T., Fráter-Bihari, P. (2025) 'Gyermejjogok az online térben', *In Medias Res*, 2025/1, pp. 117–143; <https://doi.org/10.59851/imr.14.1.7>.
- Dellato, M. (2018) 'Warning: The children's footprint beginning before birth', *New York Post*, 8 November [Online]. Available at: https://nypost-com.translate.goog/2018/11/08/warning-your-kids-digital-footprint-starts-before-birth/?_x_tr_sl=en&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=sc (Accessed: 7 July 2023).
- Gazdasági Versenyhivatal (2022) 'Tájékoztató az influenszer marketingről' [Online]. Available at: https://gvh.hu/pfile/file?path=/szakmai_felhasznaloknak/tajekoztatok/Tajekoztato_az_influenszer_marketingrol.pdf1&inline=true (Accessed: 4 November 2023).
- Gál, E.D. (2020) 'Sharenting and children's rights - the harmful effects of parents' social media use on children', *Family Law*, 2020/4, pp. 19–25.
- Government of Hungary (2017) 'Digital Well-being Programme 2.0.' [Online]. Available at: <https://www.edutus.hu/wp-content/uploads/2020/10/Digit%E2%80%A0JElat-Program-2.0.pdf> (Accessed: 2 November 2023).
- Hintalovon Gyermekjogi Alapítvány (n.d.a) 'Gyermekebarát média és reklám', hintalovon.hu [Online]. Available at: <https://hintalovon.hu/gyerekebarat-media/> (Accessed: 4 November 2023).
- Hintalovon Gyermekjogi Alapítvány (n.d.b) 'Digitális szülő', hintalovon.hu [Online]. Available at: <https://hintalovon.hu/digitalis-szulo/> (Accessed: 11 September 2023).
- Hintalovon Gyermekjogi Alapítvány (n.d.c.) 'Kik vagyunk mi?', hintalovon.hu [Online]. Available at: <https://hintalovon.hu/kik-vagyunk/> (Accessed: 12 August 2023).
- Jorge, A., Marôpo, L., Novello, A.M.C.L. (2022) 'Mummy influencers and professional sharenting', *European Journal of Cultural Studies*, 25(1), pp. 166–182; <https://doi.org/10.1177/13675494211004593>.
- Koltay, A. (2018) 'A véleménynyilvánítás szabadsága' in Jakab, A., Fekete, B. (eds.) *Internetes Jogtudományi Enciklopédia* [Online]. Available at: <https://ijoten.hu/szocikk/a-velemenynyilvanitas-szabadsaga> (Accessed: 2 November 2023).

- NMHH (n.d.a) 'Filter software products against harmful internet content, child lock', *nmhh.hu* [Online]. Available at: https://nmhh.hu/cikk/187272/Szurosszoftverek_a_karos_internetes_tartalmak_ellen_gyerekzar (Accessed: 10 October 2023).
- NMHH (n.d.b) 'Technológia és tartalom', *nmhh.hu* [Online]. Available at: <https://nmhh.hu/fogyasztoknak/internet> (Accessed: 1 October 2023).
- NMHH (n.d.c) 'A Gyermekvédelmi Internetkerekasztal feladata és tagjai', *nmhh.hu*, [Online]. Available at: https://nmhh.hu/cikk/187273/Gyermekvedelmi_Internetkerekasztal (Accessed: 1 November 2023).
- NMHH (2021) 'Digital Parenting Kutatás 7-16 éves gyermekekkel és szüleikkel', *nmhh.hu*, 28 October [Online]. Available at: https://nmhh.hu/dokumentum/224270/NMHH_PSYMA_7_16_eves_2021_KUTATASI_JELENTES.pdf (Accessed: 4 November 2023).
- NMHH (2022a) 'Kiderültek az internetezési szokások: a 2 éves gyerekek és a 85 éves idős ember is használja a netet', *nmhh.hu*, 22 June [Online]. Available at: https://nmhh.hu/cikk/229984/Kiderultek_az_internetezesi_szokasok_a_2_eves_gyerek_es_a_85_eves_idos_ember_is_hasznalja_a_netet (Accessed: 1 October 2023).
- NMHH (2022b) 'Pszichológiai, érzelmi és társadalmi károkat okozhat az online zaklatás', *nmhh*, 6 September [Online]. Available at: https://nmhh.hu/cikk/231767/Pszichologiai_erzelmi_es_tarsadalmi_karokat_okozhat_az_online_zaklatas (Accessed: 17 August 2023).
- NMHH (2023) 'Az elektronikus hírközlési piac fogyasztóinak vizsgálata – Internetes felmérés 2022', *nmhh.hu*, 28 March [Online]. Available at: https://nmhh.hu/dokumentum/237510/nmhh_internetes_felmeres_2022.pdf (Accessed: 3 October 2023).
- Országos Gyermekvédelmi Szolgálat (n.d.) 'Területi Gyermekvédelmi Szakszolgálatok' [Online]. Available at: <https://ogysz.hu/teruleti-gyermekvedelmi-szakszolgalatok> (Accessed: 1 November 2023).
- Pásztélyi E., Bordács, B. (2020) 'Competition concerns in zero price markets', *Versenytükkör: a Gazdasági Versenyhivatal Versenykultúra Központjának lapja*, 16/2, 2020, pp. 25–32.
- Ranzini, G., Newlands, G.E., Lutz, C (2020) 'Sharenting, Peer Influence, and Privacy Concerns: A Study on the Instagram-Sharing Behaviors of Parents in the United Kingdom', *Social Media + Society*, 6(4), pp. 1–13; <https://doi.org/10.1177/2056305120978376>.
- Steinberg, S. (2017) 'Sharenting: Children's Privacy in the Age of Social Media', *Emory Law Journal*, 66(839), pp. 16–41 [Online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711442 (Accessed: 6 August 2023).
- Verswijvel, K., et al. (2019) 'Sharenting, is it a good or a bad thing? – Understanding how adolescents think and feel about sharenting on social network sites', *Children and Youth Services Review*, 2019/104, 104401; <https://doi.org/10.1016/j.childyouth.2019.104401>.

Vinney, C. (2022) 'The Impact of 'Sharenting': How Much Info Is Too Much?', *verywellmind.com*, 1 November [Online]. Available at: <https://www.verywellmind.com/the-impact-of-sharenting-6361714> (Accessed: 21 September 2023).

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

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 capacity⁹. 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 authority¹⁰, and various provisions ensuring special protection for minors no longer apply to them¹¹. 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 17¹⁵. 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 crime¹⁷.

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, 442¹, 991 para 1 of PCC, and Art. 144¹ 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 Services²⁵ 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 Provision 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 generation³¹, smishing³², call line identification spoofing³³, and modification of address information³⁴ 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.

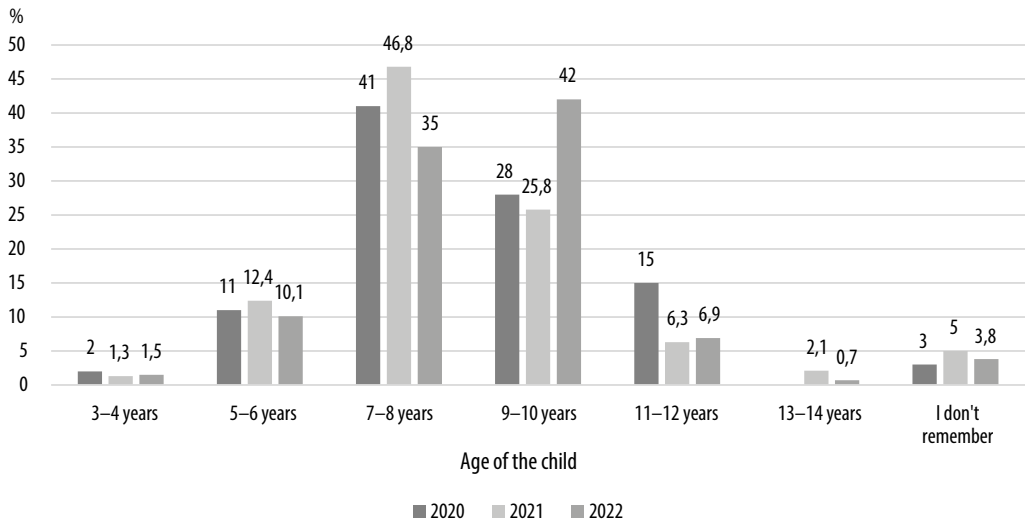
36 Ibid., p. 48.

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 phone⁴⁰



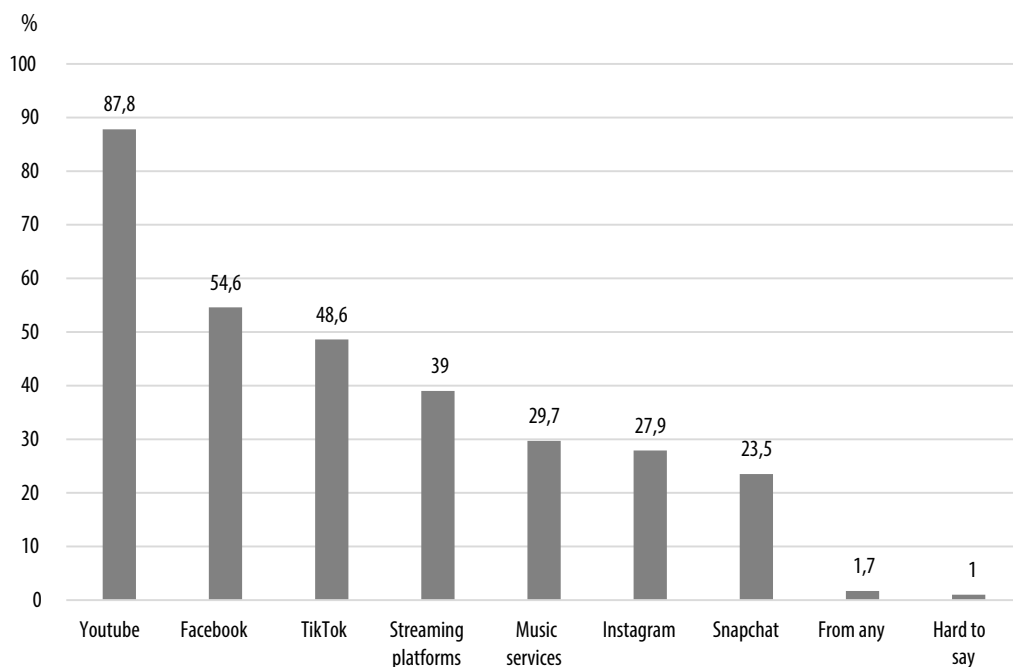
3.2. Children's Activities on the Internet

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 children⁴¹

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

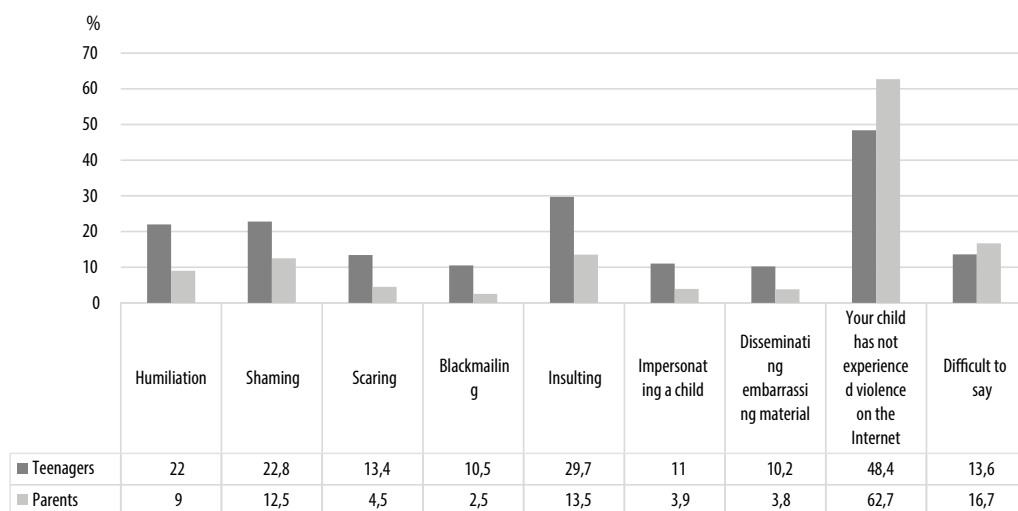
Polish adolescents are not uncritical of the Internet ecosystem and do recognise its many risks. Their primary concerns include theft and the sharing of their data, loss of financial assets, hacking of smartphones and computers, and various threats related to cyberattacks. Half of adolescents express 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). Alarming, 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 subject⁴⁷



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 nature⁵⁰ 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 abuse⁵¹ 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 Poland⁶¹ 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 2024⁶⁴, 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 property⁸². A child, like any other person, can also claim protection against defamation or insult, whether committed in the real world or online⁸³.

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 information⁸⁴. 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.⁸⁵⁸⁶

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. 216¹ 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. 216¹ 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 2010⁸⁹ 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 patostreaming¹⁰³ 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/10.1177/107780121032866>.
- 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&treaty-num=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) *Spółeczeństwo 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., Czachkowska, 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://dziekokrzywdzone.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-konsumentenckie-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).

Children in Digital Age – Romanian Perspective

Zsolt KOKOLY

ABSTRACT

The paper conducts a detailed analysis of children's rights in Romanian legislation with a special focus on their application in a digital context. As the study shows, Romania does not have extensive legislation concerning children's rights in the digital environment, and thus one of the main challenges of the study is identifying the relevant sources of law among the more general pieces of legislation and adjusting them to the digital environment. The study is structured in six chapters, where the introductory chapter presents the general legislative framework on the rights of the child in Romania, including a brief historical overview of the main milestones of the development of children's rights, concluding with an outline of the most important rights and categories of rights children enjoy according to the international and Romanian legislation.

The next chapters proceed with the analysis of six different topics, namely, the protection of children against digital harm based on the Romanian Criminal Code and the National Education Law, the review of authorities entrusted with the protection of children's rights in the digital world, the protection of children by the media law, the right of the child to be informed, heard, and express their opinion, aspects related to data protection, and finally, the state of play of the protection of children's rights in Romania's digital space.

KEYWORDS

children, Romania, children's rights, digital environment, digital harm, media law, data subjects, freedom of opinion

1. General Framework of Laws Regarding Children's Rights in Romania

Presently, the general framework of the Romanian laws concerning children's rights comprises a series of international conventions signed by Romania and adopted in the national law. The core document in the field of children's rights, the United Nations Convention on the Rights of the Child (1989), was ratified by Romania on 28 September 1990 and transposed by Law no. 18/1990.¹ The Convention has been a source of inspi-

1 Lege nr. 18 din 27 septembrie 1990 (*republicată*) pentru ratificarea Convenției cu privire la drepturile copilului*) Publicat în Monitorul Oficial Partea I. nr. 314 din 13.06.2001.

Zsolt KOKOLY (2025) 'Children in Digital Age – Romanian Perspective' in Halász, Cs. (ed.) *Children in Digital Age*. Miskolc-Budapest: Central European Academic Publishing, pp. 199–222. https://doi.org/10.71009/2025.csh.cida_10.

ration when drafting Law no. 272/2004 on the protection and promotion of children's rights,² which became the special law after its adoption governing children's best interest in Romanian national law.

The general framework of the Romanian laws concerning children's rights is completed by the constitutional provisions enshrined in the Constitution of Romania adopted in 1991 (amended in 2003)³ and the relevant articles in the New Civil Code of Romania⁴ (in effect since 2011), as well as a series of special laws containing pertinent norms.⁵ For the purpose of this country report, the provisions of two special legislative acts are of relevance: the Media Law⁶ and the adjoining Regulatory Code of Audiovisual Content,⁷ as well as the Law of National Education.⁸ Additionally, there are legal provisions comprised in the new Criminal Code of Romania⁹ that shape a system of sanctions to enable the protection of children's rights.

A first milestone in the constitutional dimension of children's rights is the enshrinement of the principle stating the "special care of children until they turn 18 years of age", introduced in 1948. The historical evolution of children's rights in the subsequent constitutions of Romania recognises several amendments, such as the protection of the interest of the mother and the child introduced in 1952 and maintained also in the 1965 version of the Constitution.

Articles 22 to 35 of the Constitution of Romania (2003) establish a general framework of fundamental rights and freedoms that affect all natural persons, thus also natural persons having the legal condition of child. These rights are as follows: the right to life, to physical and mental integrity, individual freedom, the right to defence, freedom of movement, personal and family privacy, inviolability of domicile, secrecy of correspondence, freedom of conscience, freedom of expression, the right to information, the right to education, access to culture, the right to protection of health, and the right to a healthy environment.

Article 49 of the Constitution of Romania (2003) is dedicated to the protection of children and young people, granting children and young people special protection

2 Lege nr. 272 din 21 iunie 2004 privind protecția și promovarea drepturilor copilului (**republicată**). Publicată în Monitorul Oficial Partea I. No. 159 din 05.03.2014.

3 Constituția României. (*republicată*) Publicat în Monitorul Oficial, Partea I. nr. 767 din 31 octombrie 2003.

4 Codul Civil din 17 iulie 2009 (**republicat**) (Legea No. 287/2009**) Publicat Monitorul Oficial Partea I. No. 505 din 15.07.2011.

5 A complete list of legislative acts pertaining to the protection and promotion of children's rights is published here: <https://copii.gov.ro/1/legislatie-nationala/> (Accessed: 15 March 2024). For a list of legislative acts in chronological order, see: Murgu, 2022, pp. 17–36.

6 Legea 504/2002 a audiovizualului. Publicată în Monitorul Oficial Partea I. No. 534 din 11.07.2002.

7 Decizie No. 220 din 24 februarie 2011 privind Codul de reglementare a conținutului audiovizual (modificată). Publicată în Monitorul Oficial Partea I. No. 1131 din 14.12.2023.

8 Legea 1/2011 a educației naționale. Publicată în Monitorul Oficial Partea I. No. 18 din 10 ianuarie 2011.

9 Codul Penal din 17 iulie 2009 (Legea nr. 286/2009) Publicat în Monitorul Oficial Partea I No. 510 din 24 iulie 2009.

and assistance in realising their rights. It is the obligation of the state to grant allowances for children and benefits for the care of ill or disabled children, extending social protection for children and young people also to other forms, which are established by law.

The constitutional provisions enshrined in Art. 49 forbid the exploitation of minors, their employment in activities that might be harmful to their health or morals or might endanger their life and normal development, while also forbidding the employment of minors under the age of 15 for any paid labour. Similar to the obligation of the state to provide allowances and benefits, the public authorities are bound to contribute to secure the conditions for the free participation of young people in the political, social, economic, cultural, and sporting life of the country.

In fact, stating the section on the protection of children and young people comprised in Art. 49 para. 1 enforces an exception to the principle of equality of rights, stating that citizens are equal before the law and public authorities, without any privilege or discrimination (comprised by Art. 16 para. 1). The enshrinement of this derogation is justified by the special condition children and young people have as opposed to the condition of other citizens.¹⁰

The Constitution of Romania enshrines in Art. 20 the implementation of all international and European legal documents recognising and promoting human rights, including children's rights. Art. 20 of the constitutional provisions refers to the application of international treaties on human rights, as well as precedence of law in case of inconsistencies, stating that constitutional provisions concerning the citizens' rights and liberties shall be interpreted and enforced in conformity with the Universal Declaration of Human Rights, with the conventions and other treaties Romania is a party to. In case there are any inconsistencies between the covenants and treaties on the fundamental human rights Romania is a party to and the national laws, the international regulations shall take precedence, unless the Constitution or national laws comprise more favourable provisions.

The New Civil Code of Romania (in force since 2011) represents a second pillar in the general framework on children's rights. The adoption of the new Code rendered void the Family Code, a legislative act adopted in 1953 and amended throughout 1974. After the adoption of the New Civil Code of Romania, all provisions concerning marriage, divorce, and child protection became part of the Civil Code.

The New Civil Code offers a definition for the notion of "child" (*copil*) in Art. 263, in which it formulates the principle of superiority of the child's interest. In the legal interpretation offered by the legislator, in the sense of legal provisions regarding the protection of children, the term "child" refers to a person who has not turned 18 years of age nor has gained full capacity to act according to the law.

However, the text of the New Civil Code uses the syntagm "child" interchangeably with the notion of "minor", thus offering another approach in definition, based on the capacity to act. Regarding the scope of capacity to act, Art. 38 defines full capacity to

10 Bodoaşcă, 2018, pp. 362–363.

act as starting the moment the person becomes of age and, subsequently, states that a person becomes of age when turning 18 years.

Apart from the exceptions recognised by the law, people who have not turned 14 years of age have no capacity to act, as stated in Art. 43. However, the law recognises exceptions where capacity to act is granted to persons who have not turned 18 years of age (the case of the married minor or the case of anticipated capacity to act, both cases pertaining to persons who have turned 16).

Art. 41 defines the concept of partial capacity to act, granting it in terms of age to any person turning 14 and proceeding later in Art. 42 to a description of the scope and extent of partial capacity to act. According to the legal provisions, the minor may engage in legal acts regarding work, artistic, or sporting activities, or activities related to the person's profession, having the approval of the parents or guardian and in respect of special legal provisions, if there are any. In the case detailed above, the minor acts independently upon their rights and also executes independently obligations that arise from these rights, while also being granted the liberty to dispose independently of any earned income.

For the purposes of the present report, we will use the term “child” (instead of “minor”) in the interpretation given by the New Civil Code and corroborated with the definition formulated by the special law (Law No. 272/2004 on the protection and promotion of the rights of children) in Art. 4 (a): “child – a person who has not turned 18 years of age nor has gained, according to the law, full capacity to act”.

Children are granted rights that enjoy special protection from the moment the child is conceived, under the presumption of a subsequent live birth. This principle is formulated in Art. 36 of the New Civil Code, stating that children's rights are effective from the moment of conception provided the child is born alive. This entails that children's rights are recognised from the moment of conception, but only if the child is born alive. It must be noted here that the provisions of Art. 412 on the legal timeframe of conception are to apply (establishing the legal time of conception of the child in the interval contained between day 300 and day 180 calculated from his/her birth).

This article enshrines the rights of the child from the moment they are born, stating that the person conceived must be equal with the person born in every instance that serves its interest, but on the condition that the child is born alive and has a viable existence.

The conditioning of rights to the child the moment it is conceived means that children enjoy a special protection starting at the moment of conception, but they are unable to fully access the rights conferred on them.

Presuming the child will be born alive, he has certain patrimonial and extra-patrimonial rights from the moment of conception; these include the right to inherit or the right to own goods, while extra-patrimonial rights include the right to dignity, the right to physical and psychical integrity, identity, and development.

Article 264 of the New Civil Code refers to children's rights in administrative or legal procedures concerning their person, making it mandatory that a child who has turned ten years old be heard. Moreover, should the competent authority consider

it necessary for the solution of the case, a child younger than ten years of age can also be heard. The right to be heard refers to the possibility of the child asking for and receiving any information, in accordance with his age, to express their opinion and to be informed on the consequences their opinion may cause, as well as on the consequences of any decision regarding their person.

According to this article, any child may ask to be heard, according to the provisions laid down in para. 1 and para. 2, and in case the competent authority rejects the claim, a reason for such rejection must be given. It stands to reason that the child's opinions will be taken into consideration in accordance with their age and level of maturity.

The main legislative act governing the protection and promotion of children's rights in Romania is Law No. 272/2004 on the protection and promotion of the rights of children, acting as a common frame of reference on children's rights.

At the centre of this law lies the protection and promotion of the child's best interest, the legal provisions following the provisions of the Convention on the Rights of the Child, structured in 12 chapters where each chapter comprises a set of rules on the protection and promotion of children's rights.

The dimensions of the child's best interest are confined in Art. 2, enshrining in para. 1 that the present law, any other regulations adopted in the field of protecting and promoting the rights of the child, as well as any legal act issued or, if the case, signed in this field, are subdued primarily to the child's best interests. The child's best interest is seen as adjacent to the child's right to a normal physical and moral development, to socio-emotional equilibrium, and to family life. The principle of the child's best interest governs the rights and obligations the child's parents have and their other legal representatives, as well as any other person who is lawfully entitled to care for the child. Also, the principle of the child's best interest prevails over all proceedings and decisions regarding the child made by public authorities and authorised private entities, as well as in cases argued in front of court authorities. People involved in the activities detailed above must involve the family in all decisions, actions, and measures regarding the child and must ensure the care, upbringing, formation, development, and education within the family.

In determining the child's best interest, a set of criteria may be taken into consideration, such as the need for physical, psychological development, for education, health, security, stability and adhesion to a family; the child's opinion, depending on their age and stage of maturity; the evolution of the child, especially in cases of abuse, negligence, exploit or any other form of violence on the child, as well as potential situations of risk that may arise in the future; the capacity of the parents or the people who will raise and care for the child to respond to the child's concrete needs, as well as maintaining personal relationships with people the child has formed relations of attachment.

Based on the legal interest at their centre, the rights comprised in the legal framework offered by Law No. 272/2004 on the protection and promotion of the rights

of children can be categorised into rights to development, rights to protection, and rights to participate.

The rights to development refer to the satisfaction of basic needs, including the need to develop personality traits and mental and physical abilities. The main rights granted by the law in this category are the right to development, the right to education, the right to medical care, the right to social assistance, and the right to play.

The legal provisions regarding rights to development include the child's right to be brought up in a family alongside their parents (Art. 35), with both parents bearing the responsibility for the upbringing of the child (Art. 36). Parents need to take into consideration the child's capacities to develop, corroborated with their rights to participate. The state has the responsibility to assist the parents in their mission regarding the upbringing of the child by ensuring the network of facilities, such as schools, hospitals, and other institutions.

Some of the rights to development include the child's right to be brought up in conditions enabling his physical, mental, spiritual, moral, and social development (Art. 37); the child's right to benefit from a lifestyle permitting their physical, mental, spiritual, moral, and social development (Art. 47); the child's right to receive an education stimulating the development of their abilities and personality without discrimination (Art. 51); and the child's right to rest and vacation (Art. 53).

Rights of protection comprise another category of children's rights formulated in the special law. These rights serve the purpose of insuring children against situations of risk, such as illegal transfer abroad, violence, abuse, or negligence from the parents or guardians, sexual or other kinds of abuse, implication in illegal substance traffic, and human trafficking. Protection rights also encompass a series of measures pertaining to the relation of the child with their family, as well as the case of children in vulnerable situations.

Rights to protection refer to abuse, negligence, exploitation, trafficking, illegal migration, abduction, violence, and internet pornography, as well as any other form of violence, regardless of the environment: family, institutions of education, healthcare providers, protection services, locations investigating criminal acts and rehabilitation/detention, the Internet, mass media, workplaces, sports facilities, or community centres, etc. (Art. 89).

Rights to protection refer to exploiting children by prohibiting forced labour or forced domestic activities, the prohibition extending also to educational institutions, special protection, re-education, and detention, or the cultural, artistic, sporting, publicity, and modelling environment, which bears a potential risk or is susceptible to compromising the child's education or damaging their health or physical, mental, moral, or social development (Art. 91).

The prohibition against exploiting children is formulated also in Art. 110, which expressly refers to any form of exploitation, such as illicit transfer of the child and failure to return, sexual exploitation and sexual violence, child abduction and child trafficking in every form and purpose, forced development of children's talents

damaging the optimal course of their physical and mental development, exploitation by mass media, or exploitation in the framework of research or scientific experiments.

Art. 95 forbids any kind of violence on children, as well as depriving children of their rights so as to jeopardise their life, physical, mental, spiritual, moral, or social development, or their corporal integrity or physical or psychical health, both inside the family and in institutions of protection, care, and education of children; in healthcare and educational facilities; and in any other public or private institution providing services for or conducting activities with children.

Protection rights also govern the relationship between children and their parents, as children have the right to identity: to a name, to citizenship, and if possible, to know their parents and be brought up by them (Art. 9) or to have personal relationships with and direct contact with their family, relatives, or other people they are attached to emotionally (Art. 17).

Children have the right to protect their own image and their intimate, private, or family life (Art. 27), as well as the right to have their personality and individuality respected (Art. 32).

The third category of children's rights warranted by the special law refers to the rights of participation, offering children the possibility to have a say in matters pertaining to their lives. These rights offer children the possibility to express their opinions and to discuss problems they consider of importance, as well as the opportunity to search and receive information they consider relevant for them. Romanian law explicitly grants children freedom of expression and, as a separate right, the right to freely express opinions in matters pertaining to them in legal and administrative procedures.

Participation rights have limitations, as children need to be capable of forming their own opinions to express and exert them; however, this does not mean by any chance that young children are not entitled to participation rights, as they have their own needs and capacities for participation. The right to participate must be corroborated with age limits set out by legal norms, with Romanian law granting children over ten years old the right to be heard in all legal and administrative procedures concerning them. Even children younger than ten may be heard if the competent authority deems it necessary, and their opinion can be taken into consideration based on their age and level of maturity. Generally, as the child grows older, they will have more and more participative needs, and they will be more and more capable of forming and expressing their own opinions.

The category of participative rights encompasses key rights for children, such as the right to freedom of expression, as well as to seek, receive, and promote information, as granted by Art. 28; freedom of thought, conscience, and religion (Art. 30); freedom of association, in formal and informal structures, as well as the right to freedom of peaceful assembly, within the limits stipulated by the law (Art. 31); and the right to file complaints on its own regarding the violation of his fundamental rights (Art. 34).

Children belonging to a national, ethnic, religious, or linguistic minority have the right to their own cultural life, to declare their ethnic and religious affiliation, and to practice their religion, as well as the right to use their language with other members of the community to which the children belong.

Law no. 272/2004 on the protection and promotion of the rights of children has been revised several times, the most recent amendments being introduced in 2022.

Amendments refer to the freedom of information, including that in online environments (Art. 28); attributing to the child protection services institutional network the responsibility to act promptly in instances where the child's development is jeopardised (Art. 41); and the introduction of health education classes in schools, starting with the eighth grade (Art. 46). The introduction of bullying, including cyberbullying, as a phenomenon of psychological violence on children in educational institutes (Art. 52) is the consequence of the amendment of the Law of National Education to comprise measures on violence, including physical and psychological violence (bullying and cyberbullying) as well as emotional abuse.

2. Special Legal Regulation Regarding the Protection of Children Against Digital Harm

Children represent a group considered more vulnerable against digital harm than the average group of citizens (the typical consumer/data subject), as young children or the elderly may not have the necessary digital skills or know their rights in the digital environment. Children can be affected by two types of vulnerability: inherent vulnerabilities that arise from neediness and dependence on others, and situational ones that appear in specific circumstances or situations.

The legal framework on measures to combat digital harm to children mainly includes legal provisions from the current (new) Romanian Criminal Code. Phenomena such as cyberbullying, grooming, sexting, sextortion, online identity theft, personal data theft, online hate crimes, abuse of one's image, etc. that are usually associated with the concept of digital harm against children must be corroborated with the existing regime of criminal acts stated in the Code and assimilated with one or several of the criminalised behaviours.

There are some manifestations of digital harm to children that have a sanctions regime outside the scope of the Criminal Code too: the phenomenon of cyberbullying in educational facilities is regulated in the Law on National Education, while failure to observe rules regarding the participation of children in audiovisual media programs or the labelling and content rating of audiovisual media content to respect their mental and psychological development is regulated in the Media Law and the Regulatory Code on Audiovisual Content.

Cyberbullying is defined in the annex on methodology and action plan completing the Law on National Education as follows:

‘Psychological violence in cyberspace, or cyberbullying, comprises actions conducted relying on internet networks, computers, tablets, and mobile phones, and it can contain elements of online harassment, combining illicit and/or offensive content that refers to any behaviour transmitted by means of technology, as identified on social media, websites, and messaging. This form of violence is not limited to repeated behaviour regarding mails, posting messages, images, or videos with abusive/belittling/offensive content, including here also the deliberate exclusion/marginalisation of a child in online environments or hacking personal email passwords as identified in online groups of social networks or other online formats of electronic communication.’¹¹

In the text of the annex, cyberbullying is discussed in the general framework of psychological violence in educational facilities, with physical violence and cyberbullying representing two forms of manifestation of the same prohibited behaviour: bullying.

The main legal source, the annex of the Law on National Education defines psychological violence as bullying through physical, verbal, relational, and/or cybernetic actions or series of actions, made intentionally and by using a power imbalance that results in violations to one’s dignity or the creation of an atmosphere of intimidation, hostility, degradation, humiliation, and offence, directed against one person or one group of persons, which leads to discrimination and social exclusion that may be linked to adhesion to a certain race, nationality, ethnicity, religion, social category or a vulnerable category, sex or sexual orientation, personal traits, action or series of actions, behaviours, taking place in educational institutes and all locations destined for education and professional development (Art. 6¹ glossary).

A 2019 survey on the state of play of children’s rights in Romania has concluded that one out of three children in junior high and high school cycles claims to have been subjected to a form of physical or psychological violence at school, and the number of students claiming to have experienced cyberbullying is even higher.¹²

Even though continued forms of bullying may have serious consequences on the mental health of students and their academic performance, there are no sanctions in the text of the guidelines to the Law on National Education for instances of cyberbullying in educational facilities, as most actions are directed to prevention. However, in cases of confirmed cyberbullying, the multidisciplinary team of the educational facility has attributes in mediation and conciliation. Administrative measures may extend only to resorting to the school statutes or the student charter, with disciplinary measures such as movement from one class to another or expulsion from the school being considered measures of last resort.

To distinguish between bullying in school and other behaviour common among children, the following elements need to be identified: intent (as bullying is always

11 Art. 1 para. c of Law on National Education.

12 Alexandrescu, 2019, p. 151.

intentional and meant to offend someone), repetitive nature (aggression is always directed against the same victim), and imbalance (in all cases, the victim is vulnerable and in no position to defend himself in the presence of an imbalance of age, personal traits, socioeconomic position, or gender).

Cyberbullying translates in the Criminal Code to several criminal acts against the freedom of person and engages the penal responsibility of the child. Children aged 14-16 may be held responsible if the act was committed with discernment, while children over 16 years old are held responsible. Actions of cyberbullying may be identified under the offences of threat, blackmailing, or online harassment with an added component of online or electronic communication. The Criminal Code identifies the constitutive feature of threat in the ability to instil a state of fear in someone (Art. 206), so threats made in jokes do not qualify as criminal acts.

Another manifestation of cyberbullying may comprise blackmail, which refers to forcing a person to do or not to do or suffer something in exchange for illicit gain for oneself or someone else; the threat to expose a real or fictitious act that is compromising for a person or for a family member is also considered a threat (Art. 207). Blackmail is easily done by use of electronic or digital technology: phone calls, social media platforms, or other online forums.

Harassment is another type of criminal behaviour that covers cyberbullying – according to the legal provisions, it refers to an act of repeatedly following without lawful ground or without lawful interest a person or a person's home, place of work, or any other place the person frequents, thus instilling a state of fear (Art. 208). Phone calls or any other communication by electronic means is also considered to be harassment if, by its frequency or content, it instils a state of fear in a person.

Actions inflicting harm on children in digital environments may also be congruent with criminal offences identified as cybercrimes (criminal acts against the safety and integrity of informatic data and systems). Hacking accounts qualifies as unauthorised access to an information system, which can be aggravated if the purpose was to obtain data (Art. 360). Online identity theft is also punishable by law as it assimilates the state computer fraud (Art. 325) – thus the act of registering and using an account on social media that is discoverable by the general public using another person's real name and providing real data pertaining to that person (information, pictures, photographs, video) qualifies as a criminal act, as confirmed by pertinent caselaw.¹³

Theft of personal data and online images is also covered by the criminal act of violating private life, where taking unauthorised photographs, images, or recordings of a person in his/her private home or recording a private conversation constitutes violation of his private life (Art. 226). The legal provision also incriminates the unauthorised disclosure, distribution, presentation, or transmission of a conversation or images realised in circumstances such as described above to a third person or to the public, as well as the use of technological devices for audio or video recording if it is

13 Decizia No. 4 din 25 ianuarie 2021 a Înaltei Curți de Casație și Justiție. Publicată în Monitorul Oficial Partea I. No. 171 din 19 februarie 2021.

meant to realise unauthorised recording of another person or unauthorised disclosure or distribution of the material.

Art. 226 was amended in 2023 to incorporate provisions relating to the phenomenon of “revenge porn”, criminalising the action of disclosing, distributing, presenting, or transmitting in any way the intimate image of a person identified or identifiable by the information provided, without prior consent, in a way that provokes psychological pain to the person concerned or represents a violation of his image.

While the acts described above do not distinguish between adult and child victims, there are criminal acts that refer explicitly to children. For instance, the phenomenon of grooming corresponds to the factual state of sexually corrupting a child (Art. 221) or that of exploiting the child for sexual purposes (Art. 222). In these cases, the legal provisions establish a clear age limit that sets stricter age limits, incriminating acts made by an adult who persuades a child under 13 years of age to engage in sexual acts with him, even if the persuasion was made by means of transmission at a distance.

The strictest punishment from the sphere of activities that may inflict digital harm on children is stated in the article referring to child pornography (Art. 374). Production, possession with the aim of exhibition or distribution, acquisition, storage, exhibition, promotion, distribution, or providing any type of pornographic material featuring children is punishable by law. Stimulating or recruiting a child to participate in pornographic shows or watching pornographic shows with the participation of children is assimilated into the previously described situation.

Other types of activities that may cause harm to children in a digital environment are covered by regulatory regimes under the notion of hate speech or enticement to discrimination (Art. 369).

3. The State System – Authorities With Responsibility for Protecting Children’s Rights in the Digital World

The protection and promotion of children’s rights in Romania is sustained by a network of multiple pillars, comprising the national regulatory authority, central public authorities, local authorities, and specialised bodies with attributes in this field.

The main institutions with responsibilities for protecting children’s rights are the National Authority for the Protection of Children’s Rights and Adoption (NAPCRA),¹⁴ which is the Romanian central authority within the field of children’s rights, completed by a network of central and local public authorities: the general directorates for social services and child protection,¹⁵ the councils for the protection of children’s

14 Autoritatea Națională pentru Protecția Drepturilor Copilului și Adopție (ANPDCA).

15 Direcțiunea Generală pentru Asistență Socială și Protecția Copilului (DGASPC).

rights¹⁶ (both operating at the county level), and the Public Social Services Departments¹⁷ (operating at the community level).

As the central authority, NAPCRA ensures the following, applies the national legislation within the field of children's rights at the national level, and coordinates the activities developed by public or private bodies in the same field.

The authority provides representation of Romania abroad while taking necessary measures to provide the transposition of international legislation into the national legislation. NAPCRA monitors and controls the way children's rights are respected at the national level and provides recommendations to central or local authorities with regard to the measures to be adopted in this respect.

While NAPCRA acts as the national regulatory authority in the field of protecting and promoting children's rights, there are several other national institutions or central authorities with attributes in the field of children's rights. The Ombudsman's Institution is a national institution for the promotion and protection of human rights, within the meaning established by the United Nations General Assembly Resolution of 20 December 1993, which has adopted the Paris Principles. One of the deputies to the Ombudsman has attributes in the field of sustaining, protecting, and promoting children's rights and is also called, in this sense, the Children's Ombudsman. It has the mission of defending children's rights until they turn 18 years old, as well as enforcing the respect and promotion of children's rights and intervening in the following cases: physical, psychic, and sexual abuse; abduction; bullying; poverty; placement home situations; school and school garden situations; integration of children with disabilities; maintaining the relationships between children and people to whom they are attached; children with parents working abroad; as well as any other situations where children's rights might be endangered (Art. 13-14 of the governing special law).¹⁸

The protection of children's rights in the digital world forms one of the core missions of the National Audiovisual Council (NAC),¹⁹ which has a dual quality, acting as the warrantor of the public interest in the field of audiovisual communication and the national regulatory authority in the field of audiovisual media programs, the scope of regulation expressly extending to online media content as the revisions and amendment of the governing special law (the Media Law). As the public warrantor, NAC has the obligation to protect human dignity, the right to one's own image, and children's rights (Art. 2 para. (e)) and has the authority to issue regulatory decisions containing binding legal norms regarding the protection of children's rights (Art. 17, para. 1, Pt. d, Subpt. 5).

The amendments to the Law of National Education in 2020 have invested in a network of educational facilities (schools, county boards of education, the county

16 Comisia pentru protecția drepturilor copilului.

17 Serviciul public de asistență socială.

18 Legea No. 35 din 13 martie 1997 privind organizarea și funcționarea instituției Avocatul Poporului*(Republicată). Publicată în Monitorul Oficial Partea I. No. 844 din 15 septembrie 2004.

19 Consiliul Național al Audiovizualului (CNA).

centres for resources and educational assistance, teacher training centres, and the Ministry of Education and Research) with the power to act on bullying and cyberbullying by implementing prevention strategies and swiftly addressing cases of this phenomenon in educational facilities.

The objective of the new methodology²⁰ included in the Law of National Education rests on four pillars, as stated in its Part One – Scope. The first objective is to help create a safe and positive environment in the educational facility, based on respect of people, non-discrimination, motivation to learn, and ensuring the well-being of children in nursery/kindergarten/school.

Its second objective is to offer a working instrument for professionals working with children in nursery/kindergarten/school, families of children, authorities responsible for protecting children against any form of violence, including psychological violence such as bullying, as well as specialised service providers for the rehabilitation of victimised children, witnesses, and/or children with aggressive behaviour.

The third objective is to promote activities to prevent and eliminate any form of bullying and cyberbullying in the pre-university educational system, while the fourth objective is to prevent, identify, signal, and intervene with a multidisciplinary team in cases of psychological violence such as bullying and cyberbullying.

4. Legal Practice Related to the Coming of Age of Children's Rights In Audiovisual and Online Environments

The Media Law governing audiovisual and online media content contains provisions referring to the protection and promotion of children's rights, including a separate chapter with the title "Protection of Children" (Chapter III²¹). Art. 39 of the chapter on the protection of children introduces a framework for using age-appropriate content rating and labelling of media content to prevent harm to children's development. Legal provisions in place state that audiovisual media content providers under Romanian jurisdiction offering audiovisual media services that may affect the physical, psychic, mental, or moral development of children may only communicate these services to the public in a way that ensures that under normal circumstances, children cannot see or hear them. Measures used in this sense include selecting the hours of broadcasting, age-checking mechanisms, or other technical measures. These measures must be proportionate to the possible negative effects of the program. The most offensive programs, such as those with unjustified violence or pornography, fall under the strictest measures.

It is forbidden to process children's personal data that are collected or otherwise generated by audiovisual media service providers for commercial purposes such as

20 ORDIN MEC No. 4.343/2020 din 27 mai 2020 privind aprobarea Normelor metodologice de aplicare a prevederilor art. 7 alin. (1¹), Art. 56¹ și ale pct. 6¹ din anexa la Legea educației. Publicat în Monitorul Oficial No. 492 din 10 iunie 2020.

direct marketing, profiling, and behaviour marketing. Media service providers must offer the public sufficient information regarding the content that may affect children's physical, mental, or moral development. In this sense, audiovisual mass-media service providers must use a system that describes the potentially harmful nature of the content of an audiovisual mass-media service; such a system may be established by media service providers by coregulation and/or autoregulation, including here codes of conduct of the European Union.

The legal norms in the Regulatory Code on Audiovisual Content reiterate in the Preamble the legal responsibility of the NAC, as the warrant of public interest, to ensure protection of the physical, mental, and moral development of children in audiovisual programs, including commercial audiovisual communications. In this sense, as the measures for the protection of children must be correlated with the fundamental freedom of expression as established in the Charter of Fundamental Rights of the European Union, these measures enable the use of parental control or a program labelling system and the prohibition on distributing pornographic content.

The Regulatory Code on Audiovisual Content establishes different regimes for managing children's right to privacy in audiovisual media content: children younger than 14 years, children between 14 and 16 years, and children between 16 and 18 years. These age distinctions derive their legal basis from the principle of capacity to act as described in the New Civil Code.

Chapter I (Respecting children's rights in audiovisual programs) of Title II (Protection of children) comprises concrete measures relating to the obligations of media service providers relevant to the participation of children in media programs.

Article 4 details the legal norms governing the representation and participation of children of 14 years or younger in media programs, forbidding the broadcast of any indication that might lead to the identification of a child up to 14 years old if they are the victim of sexual abuse, if they are accused of committing a crime, or if they have been witnesses to crimes. If the child up to 14 years old is the victim of crimes other than the ones listed above or has been subjected to physical or psychical abuse, broadcasting of images of the child or its declarations is only possible after receiving the child's, parent's, legal representative's, or any other carer's consent. In situations where the child up to 14 years has been subjected by their parents or legal representatives to physical or psychical abuse, broadcasting images or declarations is possible only with the child's consent, the other parent's consent (who is not the presumed author of the abuse), or the consent of an authority responsible for the child.

Media service providers are prohibited from using reenactments of crime, abuse, or dramatic elements using children. Moreover, children up to 14 years old may not give interviews or declarations pertaining to dramatic events they witness in their community or their family (Art. 5).

The legal provisions of the Regulatory Code on Audiovisual Content distinguish between three age groups, setting different types of criteria for children under 14 years old, children between 14 and 16, and those between 16 and 18.

In the case of children between 14 and 16 who are accused of committing a crime or who are the victim of a crime or have been physically, psychologically, or sexually abused, their inclusion in news programs, debate shows, or audiovisual reportages can be made only by fulfilling all the following conditions: the written consent of the child; the written consent of the parents or the legal representative; assistance during the transmission or the recording by a parent or the legal representative, or by a lawyer in case of criminal investigation or arrest; and elimination of all elements that may lead to the identification of the child (Art. 6).

In the case of children over 16 who are accused of committing a crime, their participation in audiovisual programs requires explicit consent, written or recorded, as well as assistance by a lawyer if they are under criminal investigation, held in custody, or arrested. In the case of children over 16 who are either victims or witnesses to a crime or have been physically, psychologically, or sexually abused, the following steps are required: an explicit consent, written or recorded, as well as the elimination of all elements that may lead to the identification of the child, if requested by them, their parents, or their legal representative (Art. 6).

Generally, the participation of children in audiovisual media programs is conditioned by obtaining consent beforehand; participation of children under 14 years is discouraged, except for cultural events and sports competitions.

Chapter II of the Title on protection of children is dedicated to content rating of audiovisual media programs to protect children. The general rule is to restrict access to audiovisual media programs that may affect the physical, mental, or moral development of children either by conditioning access to the program or by broadcasting it only in the allotted timeframe based on its content classification (Art. 12).

Studio programs or live shows featuring smoking and alcohol consumption, as well as vulgar, trivial, or obscene behaviour, are prohibited from broadcasting in the timeframe between 6:00 and 20:00. It is also prohibited to illustrate information with pornographic images; moreover, the following types of productions are prohibited from broadcasting in the timeframe between 6:00 and 23:00: productions showing physical, psychological, or verbal violence in a reiterative manner or with a high level of intensity or gravity; productions showing scenes of sex, trivial, vulgar, or obscene language or behaviour; people in demeaning postures even with consent; and wrestling not regulated by national or international sport associations (Art. 18).

The scope of the classification of audiovisual programs is the protection of the child and providing information to the public regarding the content of the program. Content rating is conducted according to several criteria: frequency, nature, and techniques of violent scenes, especially if children are featured in them; sexual content; characters represented; and their typology and relation to violence (Art. 19 through Art. 28).

The content rating of programs follows a more nuanced age-limit structure than the one presented in the chapter relating to the participation of the child in audiovisual media programs, as it establishes six categories of content rating systems: programs suitable for all ages (no restrictions or warning signs); programs where

parental guidance is recommended for children up to 12 years old (AP label); programs forbidden for children under 12 (labelled “Progame 12”, broadcast after 20:00 o’clock), programs forbidden for children under 15 (labelled “Progame 15”, broadcast after 22:00/23:00 o’clock); programs forbidden for children, other than pornographic programs, such as horror movies, erotic movies, extreme violence, programs sponsored by alcohol producers (labelled “Progame 18”, broadcast only between 1 and 6 o’clock); pornographic programs (labelled “Progame 18+”, broadcast only between 1 and 5 o’clock under certain conditions).

News programs are also subject to certain criteria regarding protection of children and must use different means to mitigate potential risk to children, such as verbal and written warnings before scenes containing graphic descriptions or upsetting content, or delaying techniques when broadcasting live other than news and sports transmissions (Art. 29).

5. The Right of the Child to Be Informed, Heard, and Express His/Her Opinions

Articles 28 through 29 of Law 272/2004 on the protection and promotion of children’s rights create a framework for the optimal exercise of participation rights. The dimensions of the child’s right to actively participate in matters implicating him are conferred by the interplay of three adjoining rights under the greater umbrella of freedom of expression, that is, the child’s right to information on all matters of interest to them, the child’s right to be heard in all matters affecting him, and the child’s right to freely express his opinion in all matters affecting him.

Para 1 of Art. 28 confirms the freedom of expression granted to children in an indiscriminate manner. Besides the general principles regarding freedom of expression, this article has been amended in 2022 to contain *expressis verbis* provisions referring to the online format, thereby assimilating the online environment with the traditional forms and channels of expression.

The legal provisions state that the child has the right to freedom of expression. Moreover, the freedom of the child to seek, receive, and transmit information of any kind, including in online format, regarding the promotion of his social, spiritual, and moral well-being, physical and mental health, by any means and any methods of his choice, is inviolable. Parents or other legal guardians of the child, the persons who are legally responsible for children, as well as persons who, through the nature of their positions, promote and ensure the observance of the rights of children must provide information, explanations, and advice according to the children’s age and degree of understanding, as well as allow them to express their own point of view, ideas, and opinions. Also, parents may not restrict the right of the minor child to freedom of expression, except in the cases expressly stipulated by law.

The right to receive information has a corresponding part in the legal provisions, formulating the obligation of parents and guardians to provide information in a

format adapted to the understanding of the child, while also prohibiting any action by the parents or guardians that would censor the fundamental freedom of expression granted to the child.

The child's right to information covers every type and format of information necessary for his well-being, while the obligation of parents and guardians to provide the information requested also bears the necessity to adjust the information to the child's age and degree of understanding. The obligation to provide information necessary for the well-being of the child implies at the same time the responsibility of parents and guardians to shield the child from information that would have a negative impact on his development or is irrelevant or superfluous to him.

The child's right to information is protected by the greater freedom of expression, guaranteeing that he will receive all the information required without being influenced and will be able to formulate and express his own opinions.

Article 29 confirms two rights that are treated as adjoining but separate rights linked to the general notion of freedom of expression, that is, the right of the child to have the capacity to freely express their opinion in any matter pertaining to him and the right to be heard in any judicial or administrative procedure pertaining to him.

The text of the article states that the child who has the capacity to discern has the right to freely express their opinion regarding any matter that involves them. Also, the child has the right to be heard in any judicial or administrative procedure that involves him. The hearing of the child who has reached the age of ten years is mandatory. Nevertheless, the child who has not reached the age of ten years may also be heard if the competent authority deems it necessary to solve the case. The right to be heard grants to the child the possibility to request and receive any pertinent information, to be consulted, to express his opinion, and to be informed about the consequences that his opinion may generate, if observed, as well as the consequences of any decision involving him. In all legally regulated cases, the child's opinions will be taken into consideration, according to the child's age and degree of maturity.

It is the right of any child to be heard, according to the provisions of this article. If his request is denied, the competent authority will issue a motivated decision in this regard. The special legal provisions regarding the consent or the presence of the child in the procedures that involve him, as well as the provisions regarding the appointment of a curator in case of conflict of interests, are and remain applicable.

The right of the child to express his opinion on any matter pertaining to him originates from the Convention on the Rights of the Child, corroborated with legal provisions comprised in the Civil Code and other special legislative acts.

A legal analysis²¹ focusing on the nature of the two rights comprised in Art. 29 formulates several observations regarding the scope and extent of these rights. The right of every citizen to freely express his/her opinion is enshrined in the Constitution and, in this case, is assimilated with the fundamental right (freedom of expression). As such, freedom of expression is granted to every citizen and prevails over provisions in

21 Bodoaşcă and Murgu, 2020, pp. 82–84.

other legal texts. In this sense, the constitutional provision of freedom of expression extends indiscriminately to all citizens, regardless of whether they are children and regardless of whether the subject of their opinion concerns their person. Of course, the limitations to the constitutionally enshrined freedom of expression also apply in this case, as opinions expressed by the child may not violate the dignity, honour, and private life of a person, nor the right to one's own image. Freedom of expression must also respect the regime of prohibitions listed in the Constitution, that is, the prohibition of defamation of the country and the nation, calls to war and aggression, incitement to hate on the basis of nation, race, class, or religion, incitement to discrimination, territorial separatism or public violence, or obscene behaviour.

The conditioning set in Art. 29 seems to be problematic due to the potentially restrictive nature, as it limits freedom of expression based on two elements: having discernment and expressing opinions that directly have an impact on the bearer. That would imply, *per a contrario*, that a child having no discernment does not have the liberty to freely express his opinion on matters concerning him, nor in other matters that do not have a direct impact on him.

The two particularising elements in formulating the right to an opinion also contradict to a certain degree the constitutional principle granting "children and young people [the enjoyment of] special protection and assistance in the pursuit of their rights". This constitutional provision obliges the lawmaker to institute a regime favouring children's rights instead of a regime restricting them.²² An internal contradiction arises also when observing the principle of non-discrimination formulated in Art. 7, which states that children enjoy the rights conferred on them regardless of race, colour, sex, language, religion, political or other opinion, nationality, ethnicity or social origins, economic situation, type and grade of handicap, birth status or acquired status, difficulties in formation and development, or any other type of difficulty of the child, their parents, or their legal representatives.

As a *de lege ferenda* solution proposed by the legal examination cited above, the disputed provisions under Art. 29 para. 1 referring to the right of opinion could be removed, thus conferring the constitutional freedom of the child to express his opinion, including in matters that directly impact him.

Closely linked to the issue of the right to opinion is the issue of the right to be heard. The right of the child to be heard in any proceeding in front of a court of law or in any administrative procedure gives him/her the opportunity to express his/her opinion. The right of the child to be heard in legal or administrative procedures is confirmed also in the legal provisions of the Civil Code.

However, the special law 272/2004 does not confer the right to be heard to any child, only to children who have turned ten years of age, leaving the possibility to hear children younger than ten years as a facultative option. The right of the child to be heard should comprise an obligation for authorities to hear him. As the legal source formulates only a facultative option for authorities to hear children younger than

22 Ibid., p. 82.

ten years, it transpires that this right is not absolute. Moreover, while the freedom of expression is enshrined in the Constitution, there is no similar principle regarding the right of a person to be heard (the right of the child to be heard is comprised only in the special law 272/2004 and in the Civil Code). The right of the child to be heard and for his opinion to be considered, depending on his age and level of maturity, is a principle that ensures that children's rights are respected and guaranteed. The right of the child to express his opinion exceeds the coverage of the right to be heard, as the child can express his opinions in any circumstances, including legal or administrative proceedings. This thesis is sustained by the fact that unlike the right to an opinion, the right to be heard is manifested only within a legal or administrative procedure, with strict procedural rules enforced: the child acts in an official capacity (petitioner, applicant, accused, injured party, defendant, etc.), while the right to an opinion is exercised in the quality of a legal subject possessing different rights recognised by law.

The right of the child of ten years to be heard should be interpreted in a sense more resembling an obligation for authorities to hear the child in any legal or administrative procedure in matters pertaining to him. Nevertheless, children younger than ten years old can be heard too, if the competent authorities deem it necessary for the solution of the case. The right to be heard confers on the child the possibility to ask and receive information relevant to him and to be informed and consulted regarding the consequences of any decision he makes. In this framework, the opinion formulated by the child will be taken into consideration in corroboration with his age and level of maturity.

6. Personal Data and the Right to Be Forgotten

Children become data subjects when their personal data are being processed, and processing a child's personal data requires additional protection, as children are less aware of the risks and consequences of sharing data and their rights. As indicated previously, children represent a vulnerable category of data subjects, so management of their personal data presents multiple questions.

One of these questions is the problem of age: the New Civil Code confers partial capacity to act to children who have turned 14, while the regulatory framework on data protection in Romania²³ states the necessity of obtaining consent from a parent or legal guardian to enable companies to process personal data for children under 16 years old.

This raises the question of whether a child who has turned 14 may already exercise their right regarding processing their personal data and the right to be forgotten,

23 Legea No. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). Publicată în Monitorul Oficial Partea I. No. 651 din 26.07.2018.

taking into consideration also the fact that the European General Data Protection Regulation²⁴ from 2018 allows countries to provide lower ages of consent (although not below 13 years).

The Civil Code grants the child partial capacity to act, the right to independently conduct acts of maintenance and management that do not cause any prejudice to him, as well as acts like accepting an inheritance, liberalities free of encumbrances, and acts of disposition for current, small-value operations payable by the time of the transaction.

This would entail the possibility that the child who has turned 14 could already decide independently upon the processing of his personal data and right to be forgotten.

As a rule, the Romanian data protection legal framework incorporates Art. 8(1) of the Regulation (EU) 2016/679 (the General Data Protection Regulation) and requires data controllers to make reasonable efforts to verify that the person exercising the parental authority has given consent on behalf of the child: “In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child”. However, the national regulatory authority did not specify and has not issued any guidance over how the age of children should be ascertained.

This ambivalence in the age of the child data subject – and implicitly, the lawfulness of data processing – becomes more visible in the relationship between children and educational facilities, as schools collect and store a great variety of children’s personal data, where some of the data must be shared with third parties inside or outside the educational system.

7. State of Play of the Protection of Children’s Rights in the Digital Space

The UNICEF Country Office Report 2023 for Romania²⁵ stresses that despite notable progress achieved across social sectors over the years, important child rights challenges, deprivations, and inequities remain. Over 49% of children live in rural areas, with lower living standards and more precarious access to quality social services compared to the urban population. Nearly one-third of children in Romania are affected by severe material and social deprivation. Romania has the highest rate of children at risk of poverty or social exclusion in the European Union (41.5%), nearly twice as high as the EU average (24.7%, according to Eurostat 2022).

Child rights challenges persist in Romania also according to the UNICEF Country Office Report 2024: poverty risks remain high, particularly in rural areas; one in five

24 European Parliament and Council, 2016.

25 UNICEF, 2024, p. 1.

children (22.6%, Eurostat, 2023) faces severe material and social deprivation, nearly three times the EU average (8.4%).²⁶

The functioning and the efficiency of the legal framework and the network of central and local authorities having responsibilities in the field of protection and promotion of children's rights is envisioned and subsequently assessed in several policy documents comprising the national agenda in this area. The Romanian Government has adopted "The national strategy on protection of children's rights in the period of 2014-2020"²⁷ and has offered an evaluation of the results in the present policy document: "The National strategy for protecting and promoting children's rights. Safe children, safe Romania 2023-2027".²⁸

The initial document from 2014 has set out its strategic objective of promoting investments by all public authorities and public institutions in the development and well-being of children, to enforce respect for children's rights and satisfaction of their needs, as well as universal access to services. Guiding principles of the former agenda have been the focus on the development and well-being of the child, respecting and promoting the best interest of the child, the primacy of parents' responsibility in the upbringing and care of their children, and the subsidiary but responsible intervention of public authorities, while also promoting institutional partnerships with civil society. Other key aspects of the document focused on participation and consultation of children in decisions implicating them, as well as ensuring stability, continuity, and complementarity in the personalised care for each child.

Parallel to the national strategy, several projects at the national level have been either continued in amended form or launched as new initiatives.²⁹ These projects include the "Safer Internet Program" – the national platform established in Romania in 2008 with several modules, such as Ora de net (The Internet Class) Project – for the promotion of internet safety by public awareness campaigns; esc_ABUZ (escape abuse) – a dedicated hotline for receiving and managing reports and data on online illegal child sexual abuse, hate speech, and discrimination; ctrl_AJUTOR (control help) – online helpline service for reporting and dealing with harmful contact (grooming), conduct (cyberbullying) and content by one-to-one conversations with trained counsellors; Telefonul Copilului (The Child Helpline) – information, counselling, referral to the institutions able to offer the adequate assistance to each case, case monitoring, and monitoring that child rights are respected.

26 UNICEF, 2025, p. 1.

27 Anexa la Hotărârea Guvernului 1113/2014 privind Strategia Națională pentru protecția și promovarea drepturilor copilului pentru perioada 2014-2020 și Planul operațional pentru implementarea Strategiei naționale pentru protecția și promovarea drepturilor copilului pentru perioada 2014-2016. Publicată în Monitorul Oficial Partea I No. 33 din 15.01.2015.

28 Anexa la Hotărârea Guvernului No. 969/2023 privind aprobarea Strategiei naționale pentru protecția și promovarea drepturilor copilului "Copii protejați, România sigură" 2023–2027. Publicată în Monitorul Oficial Partea I nr. 942 bis din 18.10.2023.

29 Cozma, 2020, p. 3.

The current state of play referring to children accessing digital services entices new opportunities to use global resources of knowledge and connection, but there are also risks attached. The chapter dedicated to the safety of children in digital environments in the National Strategy for protecting and promoting children's rights 2022-2027 offers a list of risks, comprising exposure to content not suited to their age or to inadequate contact-inclusive abusers, forms of violence, loss of privacy due to the publishing of sensitive personal data (in public or through interpersonal communication networks), loss of control over online identity, loss of confidentiality and disclosure of information on location, or abuse with personal data resulting in negative psychological consequences. In accordance with the EU Strategy on the rights of the child, the national strategy of Romania suggests that responsibilities in ensuring a safe digital environment for children should be assumed by companies providing these services, parents and adults who have responsibilities for children's care, teaching staff, and state institutions that establish the regulatory framework and conditions for the functioning of digital services.

8. Conclusions

Children's rights, such as the right to education, to information, to free expression of opinions, to confidentiality, to play, to rest, to leisure, and to protection against all forms of exploitation, are just as relevant in the virtual environment. However, methods of guaranteeing these rights in a digital environment need to be adapted to the specifics of the virtual environment.

Studies indicate that the number of children in Romania who engage in different online activities is high, but they are very poorly or not at all protected against risks, thus resulting in negative experiences.³⁰ The number of children to have a negative experience in online environments is also high. Studies have also demonstrated that only one out of five children are subjected to parental control over audiovisual media content or restriction to use the camera; the number of children restricted from accessing social media websites may be even lower.³¹

Amending and updating the regulatory framework on the protection and promotion of children's rights and creating a substantial corpus of documents ranging from reports, surveys, studies, strategy papers, agendas, problems, and best practice catalogues and information material to sustain the decision-making process have been in the forefront of policy makers in this field. At present, general objectives in this field envision access for children to digital public services in safe conditions and

30 Strategia națională pentru protecția și promovarea drepturilor copilului "Copii protejați, România sigură" 2023–2027. Publicată în Monitorul Oficial Partea I No. 942 bis din 18.10.2023, p. 50.

31 Ibid., p. 51.

establishing specific objectives in this field, such as increasing the adult population's capacities to contribute to the safe use of virtual environments by children.

Bibliography

- Alexandrescu, G. (ed.) (2019) *Raport privind respectarea drepturilor copilului în România*. Bucharest: BMI Publishing [Online]. Available at https://avp.ro/wp-content/uploads/2020/07/raport_special_2019_2.pdf (Accessed: 15 March 2024).
- Avădanei, I., (2021) *Drepturile și siguranța copiilor în mediul online – ghidul pentru profesori*. Bucharest: Centrul pentru Jurnalism Independent [Online]. Available at <https://cji.ro/ghid-drepturile-copiilor-online/> (Accessed: 15 March 2024).
- Bodoașcă, T. (2018) *Observații critice în legătură cu egalitatea în fața legii a copiilor din afara căsătoriei cu copiii din căsătorie. Studii de dreptul familiei*. Bucharest: Universul Juridic.
- Bodoașcă, T., Murgu A.B. (2020) ‘Considerații privind libertatea copilului de a-și exprima opinia și dreptul acestuia de a fi ascultat’, *Pandectele Române*, 2020/1, pp. 80–89.
- Cozma, A. (2020) ‘Child Online Protection in Romania ITU Forum for Europe on Child Online Protection 26 – 27 November 2020’ [Online]. Available at https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2020/COP_EUR_CIS/S5%20Alexandru%20Cozma.pdf (Accessed: 15 March 2024).
- European Parliament and Council (2016) 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) [Online]. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (Accessed: 15 March 2024).
- Murgu, A.B. (2022) ‘Privire de ansamblu asupra reglementării drepturilor copilului’, *Pandectele Române*, 2022/3, pp. 17–36.
- UNICEF (2025) *UNICEF Romania – Romania Annual Report 2024*. New York: UNICEF [Online]. Available at <https://open.unicef.org/download-pdf?country-name=Romania&year=2024> (Accessed: 15 March 2025).
- UNICEF (2024) *UNICEF Romania – Romania Annual Report 2023*. New York. UNICEF. [Online]. Available <https://open.unicef.org/download-pdf?country-name=Romania&year=2023> (Accessed: 15 March 2024).

Children in Digital Age – Serbian Perspective

Sanja SAVČIĆ

ABSTRACT

In the digital age, the protection of children's rights has emerged as one of the most pressing and complex challenges facing modern societies. While fundamental human and children's rights are clearly defined through international documents such as the UN Convention on the Rights of the Child, and integrated into national legal systems like the Constitution of the Republic of Serbia, the digital environment introduces entirely new risks and opportunities for children. This calls for a reinterpretation of existing rights in the context of the internet and digital technologies, along with the development of adequate legal and institutional mechanisms for protection.

This paper analyzes the general and specific legal framework concerning children's rights in Serbia, with a special focus on their application in the digital sphere. It reviews key legal instruments – including family law, criminal law, and other specialized regulations – as well as the General Protocol for the Protection of Children, which collectively form the institutional basis for child protection. Special attention is given to rights such as the right to privacy, the right to be forgotten, the right to education and information, and the right to freedom of expression and to be heard – all of which acquire new dimensions in the digital context.

Beyond legal analysis, the paper explores the role of parents, educational institutions, and other stakeholders in the child protection system. Although Serbia has developed a relatively comprehensive institutional framework, several challenges remain – such as overlapping competencies, the absence of a specialized law on children's rights, and low awareness of digital risks among both children and adults. The paper highlights that effective protection requires not only legal regulation but also continuous education, multisectoral cooperation, and proactive engagement by all actors involved in a child's life.

In conclusion, the digital age demands a holistic approach to safeguarding children's rights, recognizing and addressing the unique risks posed by modern technologies. Despite legislative and institutional efforts, practice still reveals gaps in understanding and implementing children's rights in digital contexts – a key issue to be addressed moving forward, both in Serbia and globally.

KEYWORDS

children's rights, digital age, Republic of Serbia, child protection, privacy, right to be forgotten, internet safety, legal framework, institutional mechanisms

1. Definitions and Taxonomic Rationale

Around the world, the digital revolution has changed how people grow and mature, as well as how they build relationships and are educated. Serbia is no exception, as this global phenomenon knows no boundaries.¹ Greater Internet access across demographics, including children, is now forcing traditional societies to confront the challenges of this parallel “digital world”. Global society must balance the pros and cons of digital life, transcending national and cultural differences, especially to protect children, a particularly vulnerable group. This chapter presents the legal framework of children’s rights in Serbia.

1.1. General Regulations on Children’s Rights

It is impossible to analyse children’s rights in the digital age without referencing the United Nations Convention on the Rights of the Child (CRC), adopted in 1989 and ratified shortly thereafter by the then Socialist Federal Republic of Yugoslavia, and later in Serbia.² Thus, the CRC became an important part of Serbia’s legal system. Moreover, human and minority rights are guaranteed by generally accepted rules of international law, confirmed by international treaties, as well as laws guaranteed by the Constitution of the Republic of Serbia (“Constitution”); these frameworks are directly applied. In particular, Serbia is a signatory to two Council of Europe conventions: the Convention on Cybercrime the Budapest Convention³ and the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention),⁴ which define the legal mechanisms and instruments that states can use to combat sexual violence against children in cyberspace.⁵

The law may prescribe the manner of exercising these rights only if it is expressly provided for by the Constitution or if it is necessary for the exercise of a particular right owing to its nature. However, the law must, in no case, affect the essence of the guaranteed right. Provisions on human and minority rights are interpreted in favour of promoting the values of a democratic society, in accordance with valid international standards on human and minority rights, and in line with the practice of international institutions that supervise their implementation⁶, which specify

1 In Serbia, 86% of children and teenagers aged 9 to 17 use the Internet daily. See: UNICEF, 2023.

2 Zakon o ratifikaciji Konvencije Ujedinjenih nacija o pravima deteta, Official Gazette of SFRY – International Treaties, No. 15/90 and Official Gazette of FRY – International Treaties, No. 4/96 and 2/97. The CRC will not be analysed in detail in this chapter.

3 Zakon o ratifikaciji Konvencije o visokotehnoškom kriminalu, *Official Gazette of Republic of Serbia* – International Treaties, No. 19/2009.

4 Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog uznemiravanja, *Official Gazette of Republic of Serbia* – International Treaties, No. 1/2010.

5 Šapić, 2016, p. 2.

6 Art. 18 para. 3 of the Constitution.

the legal definition of “international law”. However, the concept of children’s rights, which began to be introduced into Serbia’s normative system after 2000, through full or partial elaboration in most laws relating to children, was confirmed by the new Constitution in 2006 and has been implemented with modest success in terms of institutional competence.

According to the Constitution, children enjoy human rights appropriate to their age and mental maturity.⁷ The Constitution guarantees the child the right to a personal name, registration in the birth register, the right to know his origin, and the right to preserve his identity. It explicitly provides for the equal status of children born in and out of marriage and protects children from psychological, physical, economic, and any other form of exploitation or abuse.⁸

1.2. Special Regulations on Children’s Rights

Soon after adopting the Constitution, Serbian lawmakers began preparing for special regulation on children’s rights, leading to the Draft Law on the Rights of the Child and the Protector of the Rights of the Child (Draft Law or DLRC).⁹ The Draft Law passed the stage of public discussion in June 2019 and was then referred to the Parliamentary Committee for the Rights of the Child, but it was withdrawn from the procedure in 2021.¹⁰ The action plan for the implementation of the Government Programme 2023–2026¹¹ does not provide for the adoption of this law either, indicating a missed opportunity to establish comprehensive and easily implementable legal regulation on children’s rights. As a result, important regulations on children’s rights remain scattered across numerous laws or simply do not exist yet.

By adopting the Family Act of 2005,¹² Serbia incorporated provisions of the CRC into its domestic legal system and became part of the global children’s rights framework. The CRC was adopted in 1989, around the time Internet providers emerged, and does not contain any reference to the digital environment, which shapes childhood today. The Serbian Family Act similarly lacks this focus. Thus, we pose the question: Does the Family Act offer a strong legal foundation for protecting children’s rights in a modern life transformed by technology? The CRC or the Family Act, in their current forms, do not address the critical questions¹³ of how to protect children’s rights in the digital environment and how to ensure children’s safety in a virtual world?

While some laws have been revised and bylaws adopted to better protect children’s rights in the digital age, with a particular focus on online peer violence,¹⁴

7 On the relationship between human rights and children rights in theory, see: Vučković-Šahović, 2001, pp. 14–19.

8 Art. 64 of the Constitution.

9 *The Draft Law on the Rights of the Child and the Protector of the Rights of the Child*. Available at: <https://www.paragraf.rs/dnevne-vesti/070619/070619-vest15.html> (Accessed: 20 November 2023).

10 Paunović, 2023, p. 9.

11 Brnabić, 2023.

12 *Porodični zakon, Official Gazette of Republic of Serbia*, No. 18/2005, 72/2011 - dr. zakon i 6/2015.

13 Šahović, 2021, pp. 165–166.

14 Dinić, 2022, pp. 39–43.

there is no specific law in Serbia regulating children's rights in the digital environment or addressing digital violence as a *sedes materie*. Other laws do contain special provisions on these issues, the most important being the Law on Primary Education and Upbringing.¹⁵ For the clear application of these provisions, the Rulebook on the Protocol of Action in Response to Violence, Abuse and Neglect was adopted in 2010¹⁶ and amended in 2020.¹⁷ These regulations express the commitment to building a system that protects children's rights and safety, as set out in the General Protocol of the Government for the Protection of Children from Violence and Neglect ("General Protocol").¹⁸ Of crucial importance is the Regulation on Safety and Protection of Children During the Use of Information and Communication Technologies¹⁹ and the Law on Special Measures to Prevent the Commission of Criminal Offences Against Sexual Freedom Against Minors,²⁰ while the Criminal Code²¹ sets out legal penalties with respect to child victims.²²

2. Children's Rights on the Internet

The most prominent outcome of digitalisation is the global network: the Internet. The Internet was created not merely for global communication and information exchange, but also exists as a "parallel world". Its initial users were assumed to be adults, but increasing technological access, especially through smartphones and PCs, has enabled children to participate online. This fact has had a dual impact on children's rights. First, children can express themselves and exercise their rights in the digital world. Second, the digital universe can endanger children's rights. The legal endeavour to shape the Internet is driven by the need to make the digital environment safe for children. In legal terms, children's rights should be protected at least as much online as they are in the physical world.

Serbia has no special legal regulation on the protection of children's rights in the digital age and no dedicated law addressing digital harm. However, this new environment and the new forms of injury it creates have been recognised by the national

15 Zakon o osnovnom obrazovanju i vaspitanju, *Official Gazette of Republic of Serbia*, No. 55/2013, 101/2017, 10/2019, 27/2018 – other law, 129/2021 i 92/2023.

16 Pravilnik o protokolu postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemari-vanje, *Official Gazette of Republic of Serbia*, No. 30/2010.

17 Pravilnik o protokolu postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemari-vanje, *Official Gazette of Republic of Serbia*, No. 46/2020.

18 Zaključak Vlade Republike Srbije 05 broj: 011-5196/2005.

19 Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnolog-ija, *Official Gazette of Republic of Serbia*, No. 13/20.

20 Zakon o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode mal-oletnih lica, *Official Gazette of Republic of Serbia*, No. 32/13.

21 Krivični zakonik, *Official Gazette of Republic of Serbia*, No. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

22 Čović, 2017, pp. 48–52.

legislature. Besides the Draft Law, existing laws do contain provisions for the protection of children in the digital environment. Moreover, many existing provisions adopted before the digital age can also be applied online.

2.1. The Constitution and Children's Rights

The Constitution includes several provisions relevant to children's rights in the digital age. Human rights, as defined in the Constitution, are directly applicable. Legislation may regulate the manner in which these rights are exercised only if explicitly provided for by the Constitution or necessary owing to the nature of the rights themselves. Such legislation must not affect or modify the essence of children's rights and protections.

According to Art. 64 of the Constitution, a child is entitled to human rights appropriate to their age and mental maturity. Every child shall be protected from psychological, physical, economic, or any other form of exploitation or abuse, regardless of whether they were born within or outside marriage. The rights of the child and their protection are to be regulated by law. According to Art. 65, both parents have equal rights and obligations to raise, support, and educate their children. However, these rights may be revoked from one or both parents only by a court ruling if it is in the best interests of the child and in accordance with the law. Art. 66 para. 1 provides for special legal protection of families, mothers, single parents, and all children, and is ensured through various laws and bylaws.

2.2. General Protocol

On 10 February 2022, the legislature adopted the General Protocol²³ to safeguard the well-being of children by preventing abuse and neglect, establishing a prompt and coordinated response to protect children from further harm, and providing therapeutic assistance to the child and their family. The General Protocol applies to all children at risk and ensures that all actions and decisions are guided by the child's best interests. Special protocols further regulate the roles and procedures for institutions such as social welfare services for children, the police, educational institutions, the healthcare system, and judicial authorities.

2.3. Family Law and Children's Rights

The Family Act is the main legislation regulating children's rights. Art. 6 of the Family Act sets out the general principle that all parties must be guided solely by the best interests of the child in all activities concerning the child. The child is not merely a family member whose interests are left to the family's discretion; instead, the child is the future of the state, and their protection serves the public interest. The state

23 See: Conclusion of the Government [Online]. Available at: <http://efaidnbmnnnibpcajpc-glclefndmkaj/>; <https://zadecu.org/wp-content/uploads/2022/03/Zakljucak-Vlade-o-usvajanju-Ops%CC%8Cteg-protokola.pdf> (Accessed: 20 October 2023); Text of the General Protocol [Online]. Available at: <https://www.paragraf.rs/propisi/opstiprotokolzazastituedeodzlostavljanjaizanemarivanja.html> (Accessed: 20 October 2023).

is obliged to take every necessary measure to protect the child from neglect, physical, sexual, and emotional abuse, and any form of exploitation²⁴, as well as measures against any individual or parent(s) responsible for such harm. The state must respect, protect, and promote the rights of the child²⁵ regardless of whether the child was born within or outside marriage²⁶. An adopted child is entitled to the same rights in relation to their adoptive parents as a biological child²⁷. The state must also provide protection for a child without parental care within a family environment whenever possible²⁸. To improve children's protection, the Family Act also guarantees rights recognised by the CRC, namely the child's right to know his origin²⁹, live with his parents³⁰, maintain relations with the parent the child does not live with³¹, proper and complete development³², education³³, undertake legal affairs (business capacity of the child)³⁴, and freely express his opinion³⁵.

2.4. Criminal Law and Children's Rights

The Criminal Code prescribes more severe penalties for crimes if the victim is a child.³⁶ Crimes committed against children are prosecuted accordingly, and punishment is prescribed specifically in these cases.³⁷

The Criminal Code also recognises digital crimes against children. For example, any person who takes a photo, film, video, or other recording of another person without their authorisation, in a way that reasonably interferes with that person's personal life, or who hands over or shows such a recording to a third party or otherwise enables a third party to access it, has committed the crime of unauthorised photography and could be punished by a fine or imprisonment for up to one year.³⁸ Moreover, whoever publishes or displays a document, portrait, photograph, film, or phonogram of a personal nature without the consent of the person involved, and thereby significantly interferes with that person's personal life, shall be punished by a fine or imprisonment for up to two years.³⁹

24 Art. 6 para. 2 of FA.

25 Ibid., Art. 6 para. 3.

26 Ibid., Art. 6 para. 4.

27 Ibid., Art. 6 para. 5.

28 Ibid., Art. 6 para. 6.

29 Ibid., Art. 59.

30 Ibid., Art. 60.

31 Ibid., Art. 61.

32 Ibid., Art. 62.

33 Ibid., Art. 63.

34 Ibid., Art. 64.

35 Ibid., Art. 65.

36 Mainly crimes against mental and physical integrity (e.g. Arts. 119/3, 121/6, 134/3 Criminal Code).

37 Arts. 180, 183, and 185 of the Criminal Code (mainly against sexual freedom). See more: Stevanović and Kolaković-Bojović, 2021, pp. 61–77.

38 Art. 144 para. 1 of Criminal Code.

39 Ibid., Art. 145 para. 1.

Displaying, obtaining, and possessing pornographic material and exploiting a minor for pornography⁴⁰ could be committed in various ways: selling and distributing pornography, using minors to produce pornography (child pornography), spreading such material, or accessing websites that host such content. The prescribed punishment is imprisonment (from six months to five years, depending on the specific offence) or a fine. Using a computer network or other technical means to commit crimes against the sexual freedom of a minor is punished cumulatively by a fine and imprisonment for up to five years⁴¹. If the victim is a child, the punishment is more severe: imprisonment for up to eight years.

Crimes against minors often provoke strong public reactions and an expectation of swift and severe punishment, especially as a deterrent. In response, the legislature adopted the Law on Special Measures to Prevent Criminal Offences Against Sexual Freedom Against Minors (hereinafter: LSM),⁴² adding an additional layer of child protection. This law prescribes special measures against perpetrators of crimes against the sexual freedom of minors specified and regulates the maintenance of a registry (“Register”) of convicted offenders, commonly known as “paedophiles”. The Register contains identifying information about each offender, including name, social security number, address, employment, distinguishing features (e.g. birthmarks, tattoos), photographs, details of the offence, sentencing history, legal consequences of the conviction, implementation of special measures prescribed by law, and DNA profile⁴³. These records are permanent and may not be deleted⁴⁴. Every person in the Register must report to the police and the Directorate for the Execution of Criminal Sanctions⁴⁵. Offenders convicted of sexual crimes against minors cannot have their sentences reduced or suspended, and they cannot be released on parole⁴⁶. There is no statute of limitations for prosecuting these crimes or executing the sentence⁴⁷. Perpetrators are prohibited from visiting or remaining in the vicinity of kindergartens or schools⁴⁸ and must seek professional counselling and keep the police informed of any intention to move or travel abroad⁴⁹. The consequences of their crimes include termination of any occupation involving collaboration or work with minors and prohibition of obtaining public office⁵⁰. Every four years from the start of the extraordinary measures, the court that made the first-instance decision decides on the need for further

40 Ibid., Art. 185.

41 Ibid., Art. 185b.

42 With the adoption of this law, part of the obligations assumed by the Council of Europe Convention on the Protection of Children from Sexual Exploitation and Sexual Abuse was implemented into domestic legislation.

43 Art. 13 LSM.

44 Ibid., Art. 14 para. 3.

45 Ibid., Art. 8.

46 Ibid., Art. 5 paras. 1–2.

47 Ibid., Art. 5 para. 3.

48 Ibid., Art. 9.

49 Ibid., Arts. 10 and 12.

50 Ibid., Art. 6.

enforcement, for up to 20 years after the sentence.⁵¹ Data in the Register is not public and is protected in accordance with data protection laws, but may be accessed by courts, prosecutors, and police when legally necessary. Authorities and entities that work with minors are obliged to request information on whether a potential employee is on the Register. In line with international agreements, this data may also be shared with foreign authorities⁵².

The protection of children's rights is a priority of criminal law. Recognising the digital world as a "way of life" – both nationally and internationally – will expand the framework for children's rights protection. In this regard, education and child-rearing laws, as well as the Rulebook on the Protocol of Action in Response to Violence, Abuse and Neglect, are particularly relevant.

3. Particular Children's Rights in Serbia

The digital world is parallel to the real world, and thus, all principles valid in the real world could be transmitted to the digital. This claim has practical value. We limit our discussion on children's rights in the digital world to the most serious issues.

3.1. *Right to Privacy and Right to Be Forgotten*

Privacy is a multifaceted concept that permeates children's family relationships, school life, friendships, entertainment, and communication, among other areas. It cannot be regulated by one law alone but requires a framework of laws depending on the specific relationships or activities relevant to the child's privacy.

The right to privacy of children is not explicitly mentioned in the Family Act but is part of Serbian law. It arises from the Constitution, which provides that children are entitled to all human rights appropriate to their age.⁵³ The Draft Law, for example, stipulates the right to privacy as the right to protection of personal, private, and family life⁵⁴. Every child has the right to be protected from arbitrary or unlawful interference with his privacy, as well as with the privacy of his family, home, and correspondence.⁵⁵ The law regulates the means and methods to protect the privacy of the child, his family, home, and correspondence. For instance, it is forbidden to expose any child to the public, through any means such as media, for any advantage, benefit, profit, or influence, or in public performances, for third parties. Participation or appearance of a child in public debates or in public media is allowed only with the consent of the child and his legal representatives⁵⁶. Despite being a draft law, its provisions are already a part of the Serbian legal system through other laws.

51 Ibid., Art. 7 para. 3.

52 Ibid., Art. 15.

53 Art. 64 para. 1 of the Constitution.

54 Art. 20 para. 1 of DLCR.

55 Todorović and Šapić, 2021, p. 10.

56 Art. 20 paras. 2-5 of DLCR.

The right to privacy, for example, is guaranteed by the Constitution in Arts. 40, 41, and 42. Art. 40 guarantees the inviolability of the home, Art. 41 guarantees the secrecy of letters and other means of communication, and Art. 42 regulates the protection of personal data. As noted earlier, the provisions of the CRC are also part of Serbian law since ratification by Serbia.

The right to privacy in the digital context is more complex, especially in relation to children. Information technologies have opened new channels of communication and enabled contact via email, chat applications, audio or video calls, and social networks, radically changing the way interpersonal relationships are established and maintained. Information technologies increasingly shape social reality, making the Internet the most frequently used communication channel.⁵⁷ The global network (or digital world) has eliminated physical boundaries and made the flow of information fast, easy, and cheap. Importantly, traditional public spaces have been replaced by Internet communities, dislocating the physical into the virtual. Privacy in the digital world is a vulnerable right. While legislation cannot reverse digitalisation, it can create a more reliable and safer world for children through new regulations, prohibitions, and restrictions. Two issues are key: regulating the accessibility of a child's life on the Internet and implementing preventive and repressive measures against harm to children's privacy.

A vast amount of children's data is uploaded by children themselves or by their parents and family members, such as photos or videos on social networks or through digital communication channels (Viber, WhatsApp, etc.).⁵⁸ While social networks require users to truthfully share their age, this method is not effective and cannot be regulated by national authorities responsible for child protection.⁵⁹ Parents, who are naturally and legally obliged to raise their children, should be aware of the potential risks to children in the digital world and take appropriate action. There is no legislation regulating children's freedom to create a digital presence. However, the Law on Protection of Personal Data⁶⁰ specifies that a minor who has reached the age of 15 can independently give consent for the processing of personal data in the use of information society services. For minors under 15 years, parental consent, or consent by the appropriate legal representative, is mandatory⁶¹. For example, educational institutions often obtain parental consent before sharing students' personal data. This law applies to personal data that is processed, in whole or in part, in an automated manner, as well as to the non-automated processing of personal data that is a part of a data collection or intended for a data collection. However, it does not apply to the processing of personal data carried out by a natural person for personal needs, i.e., the needs of his household. This latter type generates major cases of infringements of children's right to privacy. Even more problematic is when parents upload children's

57 Stepanović, 2020, p. 31.

58 Cendic, 2020, pp. 72–73.

59 Krivokapić, Adamović, 2016, pp. 209–212.

60 Zakon o zaštiti podataka o ličnosti, *Official Gazette of Republic of Serbia*, No. 87/2018.

61 Art. 16 paras. 1–2 of law on Protection of Personal Data.

private content on social networks, a practice known as “sharenting”.⁶² No law or institution protects children from parents who overshare, and most children over 15 years seldom challenge their parents.

Given the provisions on the right to erasure of personal data available on the Internet (or the “right to be forgotten”, Art. 30 LPPR), the right to privacy of children presents a vulnerability. It should be noted that the right to be forgotten is not a stand-alone right⁶³ but is linked to the right to privacy and limited to specific kinds of data.⁶⁴ The Law on Protection of Personal Data regulates this right. Under this law, a person is entitled to demand the erasure of their personal data, whether processed in an automated or non-automated manner, as part of or intended for a data collection. Minors are entitled to the erasure of personal data if such data are collected in connection with the use of information society services⁶⁵. Although the law explicitly provides the right to erasure of data only in cases where a minor of 15 years has consented to data processing, the *ratio legis* of the provision also justifies its application when consent regarding the use of information society services for a child under 15 years is given by a parent exercising parental rights or another legal representative.⁶⁶

In the case of media communication, under the Law on Public Information and Media,⁶⁷ only information from one’s private life, i.e., personal records (letters, diaries, notes, digital records, etc.), character records (photographs, cartoons, films, videos, digital records, etc.), and recorded images and voice recordings (tape, gramophone, digital, etc.), may not be published without the consent of the person whose private life the information concerns, if the person can be identified in the publication⁶⁸. A minor must not be made recognisable in information that may harm his right or interest. Consent is also required for the direct transmission of an image or voice via television, radio, and similar media. Information and records cannot be published without the consent of the person to whom they refer if such publication violates his right to privacy or any other right. Consent should be given for each publication, with the purpose and method of publication clearly stated. Consent is not valid for repeated publication or for publication in another way or for another purpose than that for which it was originally given (Art. 80). Given that the law applies only to the scope of public information, its reach is limited in the sphere of extensive

62 This practice may not be in the best interests of a child, and, therefore, the State authority has powers to regulate it. For instance, in a particular case, if “sharenting” is not in the best interests of a child, in accordance with Art. 80 of FA, the guardianship authority can perform corrective supervision over the exercise of parental rights by making decisions that warn the parents of deficiencies in the exercise of parental rights or referring them for consultation to a family counselling service or an institution specialised in mediating family relations. Kovaček-Stanić, 2022, p. 69.

63 Krivokapić, 2017, p. 12.

64 Midorović, 2019, pp. 293–296; Lučić, 2021, pp. 154–156.

65 Art. 30 paras. 2–6 of Law on Protection of Personal Data.

66 Ibid., Art. 16 para. 2.

67 Zakon o javnom informisanju i medijima, *Official Gazette of Republic of Serbia*, No. 92/2023.

68 Art. 80 of Law on Public Information and Media.

Internet communication.⁶⁹ Thus, repressive measures, particularly criminal law and its general preventative function, could play a more significant role in the protection of children's right to privacy.

3.2. *Right to Privacy and Right to Education*

The digitalisation of modern society has a profound impact on the law and its interpretation. The explanation of the right to privacy only partially reveals the complexity of the digital age. The right to education offers further insights for safeguarding the essential meaning of children's rights in this era.⁷⁰

According to Art. 71 of the Constitution, every person has the right to education. Art. 63 para. 1 of the Family Act specifically states that every child has the right to education, in line with his or her abilities, wishes, and inclinations. While primary education is compulsory and free⁷¹ in public schools, higher education is not mandatory, though still free of charge⁷². Access to higher education is granted to every person under equal conditions.⁷³ This legal framework ensures that every child has the opportunity to contribute to public and private life in the future.⁷⁴ The Constitution does not clearly define this right, particularly because the content of the right evolves with changing social and cultural contexts. Consequently, the right to education must be adapted to the digital age. Education should be understood as a process that enables children to develop professional and social competencies. The Law on Primary Education and Upbringing prescribes general cross-curricular competencies for the end of primary education and upbringing. The primary competency is to enable children to participate responsibly in a democratic society. Other competencies include aesthetic and communication competencies, a responsible attitude towards the environment and health, and entrepreneurial thinking. Digital competencies include the ability to work with data and information, solve problems, and collaborate.⁷⁵ Children must be able to communicate with others without compromising their rights. Put simply, the right to education obliges the state, educational institutions, and society to equip children with digital literacy. This encompasses technical skills, collaboration in the digital environment, understanding digital communication rules, and protecting personal data and privacy.⁷⁶

Both personal data and children's privacy are threatened in an unsafe digital environment, particularly with the rise of distance learning and online learning platforms. The COVID-19 pandemic accelerated digitalisation, revealing the vulnerabilities to children's privacy. Teachers shifted to online platforms, while parents and

69 Grigorov, 2020, pp. 113–114.

70 Đukanović and Božović, 2020, pp. 85–87.

71 Art. 5/1 of Law on primary education and upbringing.

72 Art. 71 para. 2 of the Constitution.

73 Ibid., Art. 71 para. 3.

74 Lee, 2013, p. 5.

75 Art. 21a para. 3 of Law on Primary Education and Upbringing.

76 Council of Europe, 2018.

teachers often lacked guidance on processing children's data. These problems existed even when the Law on Primary Education introduced a unique information system in education⁷⁷, which collects and processes, among other data, information on students. The Rulebook on the Unified Education Information System⁷⁸ also regulates the type of data processed and how it is managed. These regulations are harmonised with the Law on the Protection of Personal Data, but challenges remain. Although the authorisation to access data is regulated, it is unclear whether such entities are permitted, and under what conditions, to demand the erasure or modification of data.

3.3. Right to Information and Right to Education

Education in the digital age cannot be separated from the global network. Digital competence drives education, reflecting the essential value of our era: information. Art. 51 of the Constitution guarantees the right to information, entitling every individual to be informed truthfully and completely, in a timely manner, about matters of public importance. The public media are obliged to respect this right. The right to information also includes the right of every individual to access data held by state authorities and organisations entrusted with public authority, provided such data has public relevance. Special laws regulate this right and obligation. However, the right to information in the digital age extends beyond explicit constitutional provisions. It must include the environment in which information is disseminated and, regarding children, material of social, cultural, and scientific value.

Naturally, freedom of the media and the right to information are functionally connected. Art. 50 of the Constitution, titled "Freedom of the Media", states that every citizen has the freedom to establish newspapers and other forms of public media without prior permission, in a manner defined by the law. The same applies to establishing television and radio stations. The Law on Public Information and Media, the main regulatory framework, includes provisions for the special protection of children.⁷⁹

To protect the free development of children's personalities, the content and distribution of media should not harm their moral, intellectual, emotional, or social development⁸⁰. Printed media with pornographic content must not be publicly displayed in ways accessible to minors. If printed media contain pornographic content, neither the front nor back page may include it; such publications must display a visible content warning and age disclaimer. The provisions of the special law on electronic media also apply to pornographic audio and audio-visual content, including content

77 Art. 175 para. 1 of Law on Primary Education and Upbringing.

78 Pravnilnik o jedinstveno informacionom sistemu prosvete, *Official Gazette of Republic of Serbia*, No. 81/19.

79 Arts. 88, 89, 91/2, 112, 113/2, 152/1/3 of LPIM.

80 Art. 77 of the LPIM.

distributed online⁸¹. When a minor is included in information, he or she must not be identifiable, ensuring his or her rights and interests are safeguarded.⁸²

These regulations focus mainly on shielding children from harmful content, but they do not address access to beneficial content. Legislators have recognised the need to regulate children's right to information in a more affirmative manner: Art. 24 of the Draft Law prescribes the obligation of public entities, as well as other legal and natural persons, to enable and encourage access to information (domestic and international) that could help improve, realise, and protect children's rights. The nature of such content is left to the editorial policy of the media. Importantly, Internet platforms (including social networks) are not considered media under this framework and, therefore, are not subject to these provisions.

Despite the digitalisation of education and the Internet as the primary source of information, children and even adults find it difficult to navigate vast amounts of content and identify relevant information. Much online content is created by adults for adults. This makes digital literacy an even more essential educational goal. Educators must provide children with the knowledge, skills, and attitudes necessary to use digital technology effectively and safely in an environment flooded with data. Children must be able to process this data to perform various tasks, solve problems, communicate with others (online or offline, or even with machines such as artificial intelligence), manage collected information, create and share content, and build knowledge. These activities must be carried out efficiently, with autonomy and a critical mindset, in both professional and private contexts.⁸³ In this regard, education should be a joint endeavour between institutions and parents, particularly since children now spend more time online than they do in schools. This makes it challenging to clearly separate education and upbringing, requiring parents to be more involved in their child's education. Given the overwhelming volume of data children are exposed to, both educational institutions and parents must empower children to access and use relevant information safely and effectively.⁸⁴

3.4. Freedom of Expression and Right to Be Heard

The Internet provides vast amounts of information with educational potential. In terms of a child's personal development, the information capacity of the Internet enables children to make decisions, form opinions, and participate in social, educational, and cultural activities.⁸⁵ Therefore, children's freedom of expression carries significant weight in the digital environment.

Art. 46 para. 1 guarantees freedom of expression, as well as the freedom to seek, receive, and impart information and ideas through speech, writing, art, or by other

81 Ibid., Art. 78.

82 Ibid., Art 80 para. 2.

83 Gillett-Swan and Sargeant, 2018, pp. 122–123.

84 Ibid., p. 125.

85 For more details on impact of digital platforms and social media on the freedom of expression in Serbia, see: Savčić, 2021, pp. 115–122.

means. To clarify this provision in relation to children's competence, Art. 65 para. 1 of the Family Act provides that a child who can form his own opinion has the right to freely express that opinion. Accordingly, all the information a child needs to form his opinion must be made available to the child.

Beyond the general framework in the Constitution that defines the range of rights and freedoms of children in line with their competence,⁸⁶ the Family Act further specifies that freedom of expression includes the right to be heard. This right applies in all matters concerning the child and in all proceedings in which his rights are at issue, in accordance with the child's age and maturity^{87,88}. Furthermore, the Family Act explicitly states that a child who has reached the age of 10 may freely and directly express his opinion in any judicial and administrative procedure concerning his rights.⁸⁹ A child aged 10 or older may also seek redress from a court or administrative body to exercise his right, either independently or through another person or institution.⁹⁰ The court or other body is not obliged to accept the child's opinion, but any decision that differs from the child's expressed view must be clearly argued.

The right to be heard is not merely an affirmation of respectful treatment towards children; it has further practical implications. It enables adults to better represent a child's interests, which depends on the right to be heard. Adults need to understand how children perceive their problems, but more importantly, how they view potential solutions to different issues. The current situation in Serbia is not encouraging: children are rarely involved in decision-making and public policy. One reason is the complexity of such participation,⁹¹ given the diversity of children's age, family, social, cultural, and economic backgrounds. However, the predominant obstacle is the significant influence of adults.⁹² Children come from different social environments that shape their values and attitudes in different ways, so issues of interest to children can vary widely.

Participation requires a certain level of capacity from the child⁹³ and is, therefore, of exceptional interest to policymakers concerned with children's rights. Nevertheless, neither the Law on the Elementary Education System and Upbringing nor the Law on the Higher Education System and Upbringing explicitly address children's participation. While these laws contain provisions on student parliaments or other forms of assembly, they do not establish a clear stance on students' participation in policymaking and decisions related to children's matters. In other words, there is no special article that enshrines the principle of participation as a general principle of action in all situations concerning children within the education system. Since

86 Kraljić and Drnovšek, 2022, p. 109.

87 Jugović, 2021, p. 23.

88 Art. 65 para. 3 of FA.

89 Ibid., Art. 65 para. 4.

90 Ibid., Art. 65 para. 5.

91 Centar za prava detet, 2020.

92 Pešić, 1999, p. 38.

93 Novaković, 2012, pp. 192–195.

schools regulate student parliaments independently, the nature and content of participation vary.

In conclusion, apart from rules concerning children's position in various proceedings, there is no reliable mechanism to uphold the right to be heard. The Citizen Protector of the Republic of Serbia has established a panel of young councillors, and the Citizen Protector of the Province of Vojvodina has formed the Children's Council. These bodies recognise the need for children's participation in public policy, opinion-forming, and decision-making. However, their results remain ambiguous. Society, especially the youth, remains largely unaware of this right – whether due to ignorance or the limited impact of children's opinions.

4. Institutional Framework and Measures for the Protection of Children In The Digital Age

4.1. Role of Parents

We must first recognise the complexity of protecting children in the digital environment, reach a consensus on the importance of children's safety, adopt a multidisciplinary approach to children's development and upbringing, and ensure cooperation and coordination among all stakeholders. Every stakeholder must have a clear understanding of their role in creating a trustworthy environment for children.

The key stakeholder is the parent, who is not just a biological relation but is also legally bound to their child and obliged to protect him in both traditional and digital contexts. Parents must understand their role in a digitised world, where children live with and through devices that provide unrestricted access to digital content and communication. Parents can influence how and for what purpose digital devices are used. They should be more active online and know how to use other digital technologies (e.g. computer games).⁹⁴ They should set time limits for digital activity and restrict access to certain content.⁹⁵ They must also be observant enough to notice any changes in their child's behaviour and address any problems before it is too late.

4.2. Role of Educational Institutions

School is a “second home”, making educational institutions important actors. They have a significant impact on the socialisation of children. Both kindergartens and schools (particularly schools) are places where children interact with people beyond their families and with individuals for whom they are not the most important or beloved beings. Here, children develop their social skills and form their personalities. Schools have the capacity to foster tolerance and respect among children. Educational

⁹⁴ Kuzmanović et al, 2019, p. 38.

⁹⁵ Research shows that parents, owing to concerns about harmful consequences, strictly limit their children's use of technology. However, risk avoidance is different from harm avoidance. A singular focus on avoidance of risk online means that parents may be compromising the digital literacy and skills of their child – a requisite in modern life. Kuzmanović et al., 2019, p. 42.

institutions should also help children learn to respond to routine challenges and embarrassment – both offline and online. Education laws and the Rulebook on Procedures in the Institution in Response to Violence, Abuse and Neglect (“Protocol Rulebook”) provide for the prohibition of all forms of violence in educational institutions.⁹⁶

Violence and abuse can take physical, psychological (emotional), social, and electronic forms. The Protocol Rulebook states that information technologies can be considered abusive if their use causes injury to another person or endangers their dignity, regardless of how the abuse occurred (e.g. through email, SMS, MMS, websites, chat platforms, including forums and social networks). Every educational institution in Serbia is obligated to establish a special team for protection against discrimination, violence, abuse, and neglect. The team is required to ensure preservation of children’s rights in the institutional setting,⁹⁷ especially through a plan that is consistent with the Rules of Conduct.

According to the Rules of Conduct, the prevention of violence, abuse, and neglect consists of measures and activities that create a safe and stimulating environment in the institution and foster an atmosphere of cooperation, respect, and constructive communication. Intervention consists of measures and activities that cease such harm, ensure the safety of participants (i.e. victims, offenders, and witnesses), reduce the risk of repetition, mitigate the consequences for all participants, and monitor the effects of the measures taken.

Whenever suspicion arises or there is awareness that a scholar is a victim of violence, the institution needs to take measures, regardless of the place where the injury occurred. This rule is of importance in the case of digital violence, which usually occurs when children are out of school.

96 Pravilniko protokolu postupanja u ustanovi u odgovoru na nasilje, zlostavljanje I zanemari-
vanje, *Official Gazette of Republic of Serbia*, No. 46/2019 and 104/2020. Note also the “Special Proto-
col for the Protection of Children and Students from Violence, Abuse and Neglect in Educational
Institutions”, the first document to directly address protection of children from violence in the
educational system, was adopted in 2009.

97 The most important are: preparation a program for protection; providing information to
scholars, employees, and parents about planned activities, and the possibility of seeking sup-
port and help from the protection team; participation in trainings and projects for developing
the competencies of employees needed for prevention and intervention in situations of violence,
abuse, and neglect; making proposals on the measures for prevention and protection, as well
as consulting and participation in risk assessment and decision making in cases of suspicion
or occurrence of violence, abuse, and neglect. Further, the team monitors and evaluates the
effects of the measures taken to protect scholars and makes appropriate proposals on the mea-
sures to the director. Since the object of the team is to prevent or solve problems, cooperation
with experts from other competent authorities, organisations, services, and the media, for the
comprehensive protection of scholars from violence, abuse, and neglect, is necessary. The team
documents, maintains, and stores all information on the activities undertaken and reports them
to the relevant experts and authorities. Naturally, parents are included in the preventive and
intervention measures and activities.

All forms of violence, including digital, as well as the measures and activities that educational institutions are obliged to implement, are classified into three levels, with the recognition that the same forms of violence can appear at multiple levels. The first level refers to less serious forms of violence, and the third level requires the activation of an external protective network and the involvement of other services and institutions.

Relating to the forms of violence and abuse that occur through the abuse of information technology and other communication platforms, the first level includes harassment via phone, SMS, or MMS; the second level includes advertising, recording, and sending videos; abuse of blogs, forums, and chats; recording, with a camera, individuals against their will; recording violent scenes with a camera; and distribution of such recordings and images; the third level includes recording of violent scenes, distribution of such recordings and images, and child pornography.

The measures to be taken depend on the level of violence and abuse. At the first level, as a rule, activities are undertaken by the class head teacher or educator in cooperation with the parent. The purpose of the planned measure is to enhance educational work with the class community, the group of students, and individually. If the measures fail and the violent behaviour is repeated, the institution intervenes with activities provided for the second or third level.

At the second level, the head teacher shall cooperate with experts (pedagogy and psychology), the team for protection, and the director for undertaking measures. Participation of parents is mandatory. If the enhanced educational work at the second level is not effective, the director initiates an educational disciplinary procedure and imposes a measure, in accordance with the law.

At the third level, activities are undertaken by the director with the team for protection, parents and competent authorities, and other organisations and services (the centre for social work, health service, police, and other organisations and services). If the presence of parents is not in the best interest of the student, that is, it can harm him, endanger his safety, or interfere with the procedure in the institution, the director informs the competent centre for social work, the police, or the public prosecutor.

Third-level violence or abuse alerts society to the seriousness of the injury or endangerment. The director of the institution must submit a report to the competent authorities, organisations, and services, and notify the competent ministry within 24 hours. Before notification, the parents should be interviewed, unless the protection team, the competent public prosecutor, police, or the centre for social work assesses that the best interests of the child may be endangered. If the violence requires immediate intervention through measures and activities, the director informs the parents and the centre for social work, which, in turn, coordinates activities with all participants in the protection process. If there is a suspicion that a violent event may have elements of a criminal offence or misdemeanour, the director notifies the parents and submits a criminal complaint to the competent public prosecutor's office, that is, a request to initiate misdemeanour proceedings to the competent misdemeanour court.

4.3. Role of Educational Institutions

In accordance with the procedures prescribed by the General Protocol, health workers participate in all stages of the child protection process, together with other services. The specific roles played by healthcare workers in such a process are defined by the Special Protocol of the Health Care System for the Protection of Children from Abuse and Neglect.⁹⁸ A child victim of violence, including violence committed in a digital environment, who, after exposing the abuse, is most often faced with misunderstanding or condemnation from the family, threats from the abuser, and inconveniences of the judicial investigation procedure, can find relief, comfort, and encouragement through regular contact with a healthcare worker whom he trusts and with whom he has already achieved good contact in a crisis. A health worker can play a very important therapeutic role in the process of psychological recovery of the child and breaking the cycle of violence.⁹⁹

The task of the police in the process of protecting children from all forms of violence is to provide security protection for the life and physical integrity of a minor who may be an actual or potential victim of any form of violence or careless treatment, as well as to determine, in each specific case, whether there are elements of criminal offence or misdemeanour that it is competent to act on. All cases of violence in which minors are potential or real victims take priority in this work. Police intervention is fast and efficient, and officers are specially trained to protect the identity of the minor victim and to conduct interviews with the victim. In the course of pre-criminal proceedings, the police cooperate with the centre for social work and all other authorised services, namely citizens' associations, in order to provide adequate protection to minors from abuse and neglect. Regarding digital violence, the Department of High Technology Crimes both detects and processes the crimes committed.¹⁰⁰

The criminal procedure in Serbia is created to protect children, as perpetrators of crime, and children as victims.¹⁰¹ With respect to the last, the Code on Criminal Procedure and the Law on minor perpetrators of criminal acts and criminal protection provide several provisions, whose aim is to protect the rights and interests of the minors in the criminal procedure. This role belongs to all entities involved in the criminal procedure. That is, when conducting proceedings for criminal acts committed that are to the detriment of minors, the public prosecutor, investigating judge, and judges in the panel will treat the victim considering his age, personality traits, education, and the circumstances in which he lives, trying to avoid possible harmful consequences of the procedure for his personality and development. Minors are

98 See: <http://www.batut.org.rs/download/novosti/Protokol%20zastite%20dece%20od%20zlostavljanja.pdf> (Accessed: 23 November 2023).

99 Išpanović-Radojković et al., 2011, pp. 64–65.

100 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, *Official Gazette of Republic of Serbia*, No. 61/2005, 104/2009 10/2023 i 10/202.

101 Zakonik o krivičnom postupku, *Official Gazette of Republic of Serbia*, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021, Art. 56, 94/2, 143/1, 162/1, 193/3,4, 304, 363/1/3.

heard with the help of a psychologist, pedagogue, or other professional. The hearing can be conducted a maximum of two times, and more times in exceptional cases if it is necessary to achieve the purpose of the criminal procedure. If a minor is heard more than twice, the judge is obliged to take exceptional care towards the protection of the personality and development of the minor.¹⁰² The procedure is urgent, and all entities that are involved in it are obliged to conduct themselves in accordance with it (Art. 157).

The Protector of Citizens is a special body that protects, promotes, and improves children's rights.¹⁰³ With its competencies, the Protector of Citizens acts on complaints from citizens and children in cases of rights violations in various areas of children's rights, or does so on his own initiative when he learns and receives information about an eventual violation of children's rights. In all procedures for controlling the work of administrative bodies, the Protector of Citizens follows the principle of the best interests of the child.

Finally, regarding the institutional framework of protection of children in the digital environment,¹⁰⁴ an important role belongs to the National Contact Centre for Children's Safety on the Internet (NCC). NCC was established in 2017 and is based on the Regulation on the Safety and Protection of Children During the Usage of Information and Communication Technologies, as part of the Ministry for Trade, Tourism and Telecommunication. Nowadays, the competent ministry is the Ministry for Information and Telecommunication. The aim of the NCC is to create a user-friendly environment for the prevention of and to respond to child endangerment in the digital environment; it provides citizens the opportunity to contact its toll-free phone number or through its online platforms Pametno I bezbedno¹⁰⁵ and Čuvam te.¹⁰⁶ Based on the application, and depending on the type of threat to the rights and interests of the child, the ministry forwards the complaint as soon as possible to the competent body^{107,108}. After receiving the application, the bodies undertake the appropriate procedure within their competence. Employees in competent institutions learn about the risks and harmful consequences that can occur when children use information and

102 Zakon o maloletnim učiniocima krivičnih dela I krivičnopravnoj zaštiti maloletnih lica, *Official Gazette of Republic of Serbia*, No. 85/2005, Art 152.

103 Zakon o zaštitniku građana, *Official Gazette of Republic of Serbia*, No. 105/2021, Art. 2 para. 4.

104 Center for Children's Right, as an association of citizens, significantly participates in the education, prevention, and protection of children's rights, particularly regarding the digital world. See: <https://cpd.org.rs/> (Accessed: 22 November 2023).

105 See: <https://www.pametnoibezbedno.gov.rs/> (Accessed: 22 November 2023).

106 See: <https://cuvamte.gov.rs/> (Accessed: 22 November 2023).

107 A competent body includes, but is not limited to, a public prosecutor, a centre for social work, an inspection for information security, the Ministry for Education, or the administrator of the website in the event that the information from the application refers to inappropriate or harmful content.

108 Art. 6 of the Regulation.

communication technologies, and are trained to aid children, in multiple ways, in the event of harmful consequences¹⁰⁹.

5. Summary

Protecting children has been a worldwide task during the whole of the last century. Adopting the CRC sheds light on the road to a unified approach to accepting children as the most valuable and vulnerable group. Even though the CRC sets children's rights, soon after its adoption, global society is faced with a new challenge: How do we make the digital world, which is truly global and unfamiliar even to adults, safe for children? By way of explanation, legal activity has intensified to assure children's rights in a world without boundaries. The goal is twofold: interpretation of children's rights in accordance with the new digital environment and combating the risks in virtual life.

Ratification of the CRC in Serbia brought a significant change in understanding children's rights. The Constitution guarantees human rights to children, in accordance with their capacity. Rights are regulated in detail through laws and bylaws, each within its *sedes materiae*. Despite the Draft Law, its eventual adoption has been put on hold. In the age of uncertainty, this approach should be considered one of inconsistency. The understanding and the thorough application and protection of children's rights demands extensive education and training, not just for competent bodies but for parents as well. Moreover, effective action requires collaboration among all institutions and persons involved in the care of the children and in their protection. Despite a well-developed institutional mechanism of protection, the full exercise of children's rights remains off the radar because the relevant competencies are scattered across different fields of care, and there exists weak awareness of the potential risk of the Internet.

109 Ibid., Art. 7.

Bibliography

- Brnabić, A. (2023) 'Akcioni plan za sprovođenje Programa Vlade 2023-2026' [Online]. available at: https://www.srbija.gov.rs/extfile/sr/686967/akcioni_plan_za_sprovođenje_programa_vlade_2023-2026_cyr5.pdf (Accessed: 2 November 2023).
- Cendic, K. (2020) 'Children's rights to privacy in times of emergency: The case of Serbia in relation to internet education technologies', *Global Campus Human Rights Journal*, 4(1), pp. 68–90; <http://dx.doi.org/10.25330/608>.
- Centar za prava detet (2020) *Sažeta analiza novousvojene strategija za prevenciju I zaštitu dece od nasilja za period od 2020 do 2023*. Belgrad: Centar za prava deteta [Online]. Available at: http://efaidnbmnnnibpcajpcglclefindmkaj/https://cpd.org.rs/wp-content/uploads/2020/06/Analiza-Strategija-za-prevenciju-i-zastitu-dece-od-nasilja_PDF.pdf (Accessed: 1 November 2023).
- Čović, A. (2017) *Prava deteta – evolucija, realizacija I zaštita*. Belgrad: Institut za uporedno parvo.
- Council of Europe (2018) *Guidelines to respect, protect and fulfil the rights of the child in the digital environment – Recommendation CM/Rec(2018)7 of the Committee of Ministers*. Strasbourg. Council of Europe [Online]. Available at : <https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html> (Accessed: 12 October 2023).
- Dinić, B. (2022) *Digitalno nasilje*. Novi Sad: Filozofski fakultet.
- Dukanović, A., Božović, B. (2020) 'Pravo na obrazovanje u praksi – Evropskog suda za ljudska prava', *Studia Iuridica Montenegrina*, 2(4), pp. 83–100.
- Gillet-Swan, J., Sargeant, J. (2018) 'Assuring children's human right to freedom of opinion and expression in education', *International Journal of Speech-Language Pathology*, 20(1), pp. 120–127; <https://doi.org/10.1080/17549507.2018.1385852>.
- Grigorov, A. (2020) 'Povreda prava na privatnost na portalima u Srbiji: studije slučaja portala Espresso I B92', *Communication and Media*, 15(47), pp. 109–136; <https://doi.org/10.5937/cm15-20143>.
- Išpanović-Radojković, V., et al. (2011) *Zaštita deteta od zlostavljanja i zanemarivanja - Primena Opšteg protokola*. Beograd: Centar za prava deteta.
- Jugović, A. (2021) *Deca I nasilje u digitalnom okruženju*. Belgrad: Centar za prava deteta.
- Kovaček-Stanić, G. (2022) 'Parental Autonomy v. Child Autonomy v. State Authority Powers', *Law, Identity and Values*, 2(2), pp. 65–83; <https://doi.org/10.55073/2022.2.65-82>.
- Kraljić, S., Drnovšek, K. (2022) 'The Implementation of the Child's Right To Be Heard: The Slovenian View', *Law, Identity and Values*, 2(2), pp. 101–117; <https://doi.org/10.55073/2022.2.101-116>.
- Krivokapić, B. (2021) 'Pojam ljudskih prava', *Strani pravni život*, 61(1), pp. 9–20; <https://doi.org/10.56461/spz17101K>.

- Krivokapić, Đ., Adamović, J. (2016) 'Impact of General Data Protection Regulation on Children's Rights in Digital Environment', *Annals: Belgrade Law Review*, 64(3), pp. 205–220; <https://doi.org/10.5937/AnalPFB1603205K>.
- Kuzmanović, D., et al. (2019) *Deca u digitalnom dobu*. Užice: Užice Center for Children's Rights.
- Lee, S.E. (2013) 'Education as a Human Right in the 21st Century', *Democracy and Education Journal*, 21(1), pp. 1–9.
- Lučić, S. (2021) 'Pravo na zaborav – uporednopravna analiza', *XXI vek – vek usluga i uslužnog prava*, 2021/December, pp. 151–166; <https://doi.org/10.46793/XXIv-12.151L>.
- Midorović, S. (2019) 'Pravo na brisanje podataka o ličnosti dostupnih na Internetu', *Zbornik radova Pravnog fakulteta u Nišu*, 58(84), pp. 281–306; <https://doi.org/10.5937/zrpfno-22953>.
- Novaković, U. (2012) 'Pravo deteta na izražavanje mišljenja' in Marković, G. (ed.) *Prava djeteta i ravnopravnost polova – između normativnog i stvarnog*. Istočno Sarajevo: Pravni fakultet, pp. 183–199.
- Paunović, J. (ed.) (2023) *Izveštaj o stanju prava deteta u Republici Srbiji 2017-2023*. Belgrade: Centar za prava deteta [Online]. Available at: <https://cpd.org.rs/wp-content/uploads/2023/06/Izvestaj-prava-deteta-2017-2023.pdf> (Accessed: 30 October 2023).
- Pešić, M., et al. (1999) *Participacija pod lupom*. Belgrad: Jugoslovenski centar za prava deteta.
- Šapić, J. (2016) *Bezbednost dece na internetu u Srbiji: izloženost bez koordinisane zaštite*. Belgrad: Centar za istraživanja javnih politika.
- Savčić, S. (2021) 'The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism in Serbia' in Wielec, M. (ed.) *The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism: Analysis on Certain Central European Countries*. Miskolc–Budapest: Central European Academic Publishing, pp. 111–140; <https://doi.org/10.54237/profnet.2021.mwsm.4>.
- Stepanović, I. (2020) *Život na internetu: parvo na privatnost I online komunikacije*. Beograd: Institut za kriminološka i sociološka istraživanja.
- Stevanović I., Kolaković-Bojović, M. (2021) 'Informacione tehnologije u službi zaštite deteta u krivičnom postupku' in Bejatović, S. (ed.) *Videolink i druga tehnička sredstva kao načini preduzimanja procesnih radnji u kaznenom postupku (norma, praksa i poželjni slučajevi širenja mogućnosti primene)*. Belgrad: Misija OEBS-a u Srbiji, pp. 61–77.
- Todorović, M., Šapić, J. (eds.) (2021) *Vodič za digitalnu bezbednost mladih – zaštita privatnosti i sprečavanje digitalnog nasilja*. Belgrad: Beogradska otvorena škola.
- UNICEF (2023) 'Safer Internet Day 2023', [unicef.org](https://www.unicef.org/serbia/en/press-releases/safer-internet-day-2023), 7 February [Online]. Available at: <https://www.unicef.org/serbia/en/press-releases/safer-internet-day-2023> (Accessed: 22 November 2023).
- Vučković-Šahović, N. (2001) *Prava deteta i Konvencija o pravima deteta*. Belgrad: Jugoslovenski centar za prava deteta.

Children in Digital Age – Slovakian Perspective

Peter KOROMHÁZ

ABSTRACT

The chapter examines the legal and regulatory frameworks that govern the protection of children's rights in the digital environment in the Slovak Republic. It explores the multifaceted risks children face online, such as cyberbullying, exposure to harmful content, and violations of privacy, while also acknowledging the opportunities for education, socialization, and personal development that the digital space provides. Emphasis is placed on the national strategy for the protection of minors in the digital environment and the analysis of the right to privacy and the right to be forgotten, the right to be heard, the right to information and the right to education.

KEYWORDS

child protection, digital environment, right to be forgotten, right to information, right to be heard

1. Introduction to the Issue

The Slovak Republic guarantees special protection for children and adolescents directly in Article 41 of the Constitution of the Slovak Republic. One may agree with Drgonec, who states that the aforementioned article guarantees general protection to all persons who have not attained the age of majority in the legal relationships with a public interest in protecting persons under the age of 18.¹ This obligation is not further specified in the Constitution of the Slovak Republic, except for a few provisions that do not address issues related to the digital environment and the associated legal challenges. Similarly, the fundamental legal statute governing family-law relationships, Act No. 36/2005 Coll. on Family and on Amendments and Supplements to Certain Acts, as amended (hereinafter, “Family Act”), does not contain provisions that reflect the need to ensure the protection of minors regarding the risks introduced by the digital era. However, special reference may be made to Article 4 of the Family Code, according to which parents have, among other things, a duty to provide a peaceful and

1 Drgonec, 2019, p. 859.

secure environment for the family, which, in the context of today's digital age, should certainly be interpreted in the context of protecting children from the pitfalls lurking in the digital environment.

The Slovak Republic has developed a National Concept for the Protection of Children in the Digital Space, which was approved by Resolution of the Government of the Slovak Republic No. 63 of 12 February 2020 (hereinafter, "National Concept for the Protection of Children in the Digital Space") and pursuant to which tasks are to be fulfilled until the end of 2025. Alongside the adoption of the National Concept for the Protection of Children in the Digital Space, the Government of the Slovak Republic also approved a corresponding action plan for the years 2020 to 2021, based on which tasks of the national concept have been recently accomplished. This procedure was followed in 2022 by Government Resolution No. 382, which approved the Action Plan to the National Concept for the Protection of Children in the Digital Space for the years 2022 and 2023. This process culminated with the approval of an action plan for the remaining period of 2024 and 2025. Fulfilment of this action plan means a conclusion to the ongoing process of legal adjustments as well as securing institutionalised protection for minors from the perils associated with the advent of the digital age. However, the National Concept for the Protection of Children in the Digital Space is not the sole and isolated document defining state responsibilities aimed at protecting minors in the Slovak Republic. It builds upon previously adopted documents and laws, including: a) the Concept of Media Education of the Slovak Republic in the context of lifelong learning approved by Government Resolution No. 923/2009 of 16 December 2009; b) Directive No. 36/2018 of the Ministry of Education, Science, Research and Sport of the Slovak Republic for the prevention and resolution of bullying in schools and educational facilities; c) Act No. 18/2018 Coll. on the Protection of Personal Data and on Amendments and Supplements to Certain Acts, as amended (hereinafter, "Data Protection Act"); d) National Strategy for the Protection of Children from Violence, approved by Government Resolution No. 24/2014 of 15 January 2014, and subsequently by Government Resolution No. 474/2017 of 11 October 2017; e) Act on the Commissioner for Children and the Commissioner for Persons with Disabilities and on Amendments and Supplements to Certain Acts, as amended (hereinafter, "Act on the Commissioner for Children").²

In the Slovak Republic, the media space is specifically regulated by Act No. 264/2022 Coll., on media services and on amendments and supplements to certain acts (hereinafter, "Media Services Act"). This legislation, enacted in 2022, repealed and replaced two previous statutes governing this area, namely, the Act on Digital Broadcasting of Program Services and Provision of Other Content Services through Digital Transmission and the Act on Broadcasting and Retransmission. The consolidation of the legislation in this area into a single code has resulted in clarification of the legislation, which we consider to be beneficial. Given that this law was adopted

2 Bacigál et al., 2020, p. 9.

after the implementation of the National Concept for the Protection of Children in the Digital Space, it reflects the need for special protection of minors.

This fact must be assessed as positive, and the adoption of the law in question may also be considered one of the significant moments in the field of protecting minors in the Slovak Republic. The fact remains, however, that this legislation does not aim to and cannot fully provide a legal framework for the existence of so-called digital platforms and the provision of services through them. Various definitions of digital platforms can be found in the literature.³ Kasenčáková defines online platforms as bilateral or multilateral marketplaces where users and platform operators meet to facilitate mutual interaction, such as the exchange of information or a business transaction, and includes, for example, Amazon, Marketplace, Bing Search, Facebook, Google Play, Google Search, and Uber among the online platforms.⁴ In our opinion, it is thus necessary to adopt further legislation that responds to the specificities associated with the use of the various digital platforms and provides effective means of protection against the pitfalls that lurk on them, particularly for their underage users.

The primary objective of the Media Services Act, as stated by the legislator, was to transpose the revised Directive on Audiovisual Media Services into the legal order of the Slovak Republic, while simultaneously clarifying the legal framework in the affected area.⁵ Respecting the wording of the Act, we conclude that the legislator has achieved the stated objective. The most significant change introduced by this Act into the legal order of the Slovak Republic is the inclusion of video-sharing platforms within the regulatory framework of audiovisual media services. This change brought about a positive qualitative shift in legal regulation, manifesting in the legal regulation of video-sharing platforms in Slovakia, to which special protection of minors secured by said Act also applies. The new legal framework thus governs the rights and obligations related to providers of video-sharing platforms as well as various content service providers in the media environment, which intersects with the digital environment. Among the outcomes of enacting this legislation is that providers of video-sharing platforms are compelled to comply with legal requirements for the protection of minors, particularly in terms of incitement to hatred, violence, or terrorism. The text of the National Concept for the Protection of Children in the Digital Space highlighted the fact that the legal regulation in Slovakia did not reflect the provisions of Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018, amending the Directive on Audiovisual Media Services, which introduced protection for minors against programmes, videos, and audiovisual commercial announcements also in relation to providers of video-sharing platforms.⁶ The adoption of the Media Services Act rectified this situation.

3 Kalesná and Patakyová, 2021, p. 26.

4 Kasenčáková, 2016, p. 65.

5 For further reference, see: the explanatory note to the Media Services Act [Online]. Available at: <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=502806> (Accessed: 20 January 2025).

6 Bacigál et al., 2020, p. 5.

The Media Services Act of the Slovak Republic establishes the rights and obligations of content service providers, which include i) broadcasters, ii) providers of on-demand audiovisual media services, iii) retransmission operators, iv) multiplex providers, v) video-sharing platform providers, or vi) other content service providers. Additionally, this Act regulates the rights and obligations of signal distributors and delineates the role and functions of the regulatory authority, namely the Council for Media Services. Broadcasters are defined as radio broadcasting service providers and television broadcasting service providers. A programme service under this law is primarily economic, which excludes those broadcasters who transmit or disseminate programme services for non-economic reasons, specifically not for the purpose of achieving business success. The above-mentioned may represent a way in which some broadcasters deliberately attempt to exclude the application of the given law to their activities. For this reason, it will be necessary to carefully observe how judicial practice addresses the assessment of whether the distribution of a programme service is taking place for economic or other reasons. Moreover, the broadcaster is editorially responsible for the programme service, which is provided via networks with the aim of informing, entertaining, or educating the public. It stipulates that the service is provided as a deliberate temporal arrangement of programmes and other components of such a service, creating a coherent, simultaneously receivable whole.

From the perspective of the legal regulation of the digital environment as it pertains to broadcasting over the Internet, the most significant provision is § 19 (3) of the Media Services Act, according to which broadcasting of programme services via the Internet is the dissemination of programme services exclusively through the Internet, known as webcasting.

Crucial in this context is the definition of an on-demand audiovisual media service. According to § 26 of the Media Services Act, an on-demand audiovisual media service is a service: primarily of an economic nature; whose fundamental purpose, or the fundamental purpose of its separable part, is to enable viewing of programmes at a time chosen by the user; provided upon the specific request of the user based on a catalogue of programmes compiled by the provider of the on-demand audiovisual media service; for which the provider of the on-demand audiovisual media service is editorially responsible; provided through a network; provided with the aim of informing, entertaining, or educating the broad public.⁷

In light of the aforementioned definitional criteria, audiovisual media services, for the purposes of the Media Services Act, can be affirmed to encompass i) services where the user autonomously selects which video or programme to watch online or through an application, and at their chosen time (various streaming services and/or television station archives), and ii) channels on platforms such as YouTube, Facebook, TikTok, Instagram, or OnlyFans, assuming they were established for business purposes or for profit-making, and meet the other previously mentioned conditions.

7 See: Mičudová, 2023, pp. 44–45.

Additionally, the Media Services Act specifically defines the term “multiplex”, which refers to a composite data stream that includes partial data streams of television or radio programming services, or other content services, including voice services configured for collective broadcasting through the appropriate telecommunications equipment. Part nine of the Media Services Act specifically addresses the protection of human dignity and humanity, as well as the protection of minors. This legal provision is an extension of the general legal regulation of personality protection, which is governed by Act No. 40/1964 Coll., the Civil Code, as amended (the “Civil Code”). The Civil Code provides protection against unauthorised intrusions into the privacy of an individual and other components of personality. Within the given legal framework of the Civil Code, a natural person is provided with certain legal remedies through which they can exercise the right to personality protection by means of state enforcement power against third parties.⁸ These are general legal remedies aimed at protecting against unauthorised interferences with personality, which are supplemented by specific legal regulations. In terms of general protection of human dignity and humanity, Section 61 of the Media Services Act prohibits broadcasters and providers of on-demand audiovisual media services from: promoting war or describing cruel or otherwise inhumane conduct in a manner that inappropriately trivialises, justifies or approves of such behaviour; disseminating or making accessible to the public information with the intent to publicly incite the commission of any of the criminal acts of terrorism or publicly approve any of the criminal acts of terrorism; promoting violence and directly or indirectly inciting violence or hatred, disparaging or defaming based on gender, race, skin colour, language, faith and religion, political or other opinion, property, health disability, age, sexual orientation, birth, national or social origin, genetic characteristics, nationality, and affiliation to a nationality or ethnic group; unjustifiably displaying scenes of real violence where the actual process of dying is improperly emphasised or where individuals subjected to physical or psychological suffering are shown, with special consideration for the victims of criminal acts or their relatives in a manner considered to be an unauthorised intrusion into human dignity.

In our opinion, it is positive that the legislator, in the given provision of the Media Services Act, opted for an illustrative (non-exhaustive) list. We believe that it would be neither possible nor practical to provide an exhaustive list of content that should not be made available by an on-demand audiovisual media service provider owing to the protection of human dignity.

For the purposes of the Media Services Act, a minor, who is entitled to special protection, is defined as a person under the age of 18 years. This legal framework thus does not reference the concept of legal majority, which is defined by the Civil Code and associated with an individual’s attainment of full capacity to perform legal acts. According to the Civil Code, legal majority is achieved either by reaching the age of 18 or, in the case of individuals older than 16 but younger than 18, by marriage with

8 Vojčík et al, 2021, p. 131.

judicial consent.⁹This creates a situation where an individual may be considered an adult under Slovak legal norms but is still accorded special, enhanced protection as a minor in terms of the Media Services Act because of their age and corresponding cognitive and volitional maturity, considered particularly vulnerable during their development. The Act primarily aims to protect minors from content in the digital space that could disrupt their physical, psychological, or moral development. In this regard, Section 62(1) of the Media Services Act imposes an obligation on broadcasters and providers of on-demand audiovisual media services to ensure that programmes or other components of programme services or on-demand audiovisual media services that: may impair the physical, psychological, or moral development of minors are accessible only in such a way that minors cannot ordinarily hear or see such programmes or other components; contain pornography or gross, unjustified violence are provided only if technical measures are in place to prevent access by minors, particularly through encryption or effective parental controls.

For content involving pornography or violence, the Media Services Act primarily anticipates maintaining a condition where minors do not have access to such content due to it being password protected. Generally, any content that might negatively have an impact on the development of minors can be broadcast between 10:00 PM and 6:00 AM, when it is assumed that minors will not have access to it. Although this assumption may not always hold true in real life, for the purposes of the Media Services Act, if a broadcaster or provider of an audiovisual media service schedules potentially harmful content during this time, they fulfil the legal obligation requiring them to make such content inaccessible to minors under normal circumstances. Additionally, outside the time frame of 10:00 PM to 6:00 AM, broadcasters of programme services are also required to consider the timing of programme scheduling in accordance with the age suitability and type of potentially harmful content contained within the programmes. However, regardless of the time content depicting pornography or gross violence is broadcast, such specifically defined content must have access blocked by technical measures.

Section 62 (2) of the Media Services Act specifically defines what constitutes the display of unjustified violence. It is understood as the dissemination in the media of reports, verbal statements, or images in such a way that violent content is unduly highlighted relative to the context of these reports, verbal statements, or images.

The Media Services Act in Slovakia also specifically safeguards minors against the processing of their personal data for commercial purposes. If a broadcaster or provider of an on-demand audiovisual media service has collected or otherwise obtained personal data of minors while fulfilling obligations related to protecting them from inappropriate content, these data cannot be processed or subsequently transferred to other parties for commercial purposes, according to Section 62(4) of the Media Services Act. Funtá and Horváth rightly point out that personal data serve as a significant input for many of the services and products offered by major online

9 See: Strapáč, 2019, p. 56.

platforms. Consequently, digital businesses aim to collect and process as much of these data as possible.¹⁰ To align services with consumer preferences, personal data are gathered and processed at an unprecedented scale and a remarkable speed.¹¹

For this reason, it is welcome that the legal framework of the Media Services Act provides special protection for the personal data of minors against processing for commercial purposes. Owing to their level of willpower and intellectual maturity, this is especially important given that minors are particularly vulnerable to practices such as targeted advertising. Furthermore, the protection of minors under the Media Services Act is ensured by requiring broadcasters and providers of on-demand audiovisual media services to determine the age suitability of the broadcast or provided programme and the types of potentially harmful content it contains. This is intended primarily to give parents or guardians overseeing the development of minors the necessary information to assess whether to restrict access to specific programmes. For these purposes, a unified labelling system defined in Act No. 40/2015 Coll., on audiovision and on amendments to certain acts, as amended (hereinafter, “Audiovision Act”), is implemented. However, broadcasters or providers of on-demand audiovisual media services may also employ an alternative accepted labelling system, but in such cases, they are required to comply with the requirements set forth by the Audiovision Act. Broadcasters are obliged to publish the age suitability label of the broadcast programme and the type of potentially harmful content it contains not only during the actual broadcasting of the programme but also during the broadcasting of trailers for such programmes, and this labelling must also be included in their own programming offer as well as in programme guides provided to third parties. Similarly, providers of on-demand audiovisual media services must publish the age suitability label of the provided programme and the type of potentially harmful content it contains in the catalogue of programmes of the audiovisual media service on demand.

The legal framework of the Media Services Act is complemented by the Audiovision Act, which further contributes to the protection of minors’ rights. This statute regulates the rights and obligations of entities operating in the field of audiovision, and it applies, among other things, to audiovisual works presented to the public in Slovakia on any medium or made available to the public from Slovak territory for a fee. This also applies to multimedia works distributed in Slovakia on any medium or made available to the public from Slovak territory for a fee.

The Audiovision Act specifically defines what constitutes an audiovisual work intended only for adults. According to Section 2(1) of the Audiovision Act, it is defined as a work that could jeopardise the development of a person under 18 years old, who is considered a minor under the law. A minor may be particularly endangered by an audiovisual work if it contains pornography or gross or unjustified violence. This assertion is similarly applicable to sound recordings of artistic performances intended only for adults and multimedia works designated for adults. The Audiovision

10 Funta and Horváth, 2024, p. 284.

11 Funta, 2020, p. 307.

Act thus directly links to the Media Services Act, which also primarily protects minors from pornography and the display of inappropriate violence. Beyond the legal provisions of the Media Services Act, the Audiovision Act creates a specific category of audiovisual works explicitly intended for children. An audiovisual work designated for children is a work that, owing to its content and character, is specifically intended for minors under 12 years old. The Audiovision Act thus creates a unique category of works that must not display gross or unjustified violence or pornography and are explicitly intended for the youngest group of children under 12 years.

In the context of current trends and threats faced by minors in the digital and media environments, the definition of a multimedia work provided by the Audiovision Act, which also extends protections to minors, is significant. According to Section 2 (11) of the Audiovisual Act, a multimedia work is any multimedia audiovisual presentation, especially a computer game or other work, which meets the following criteria: controlled by computer software; allows searching or presentation in various media forms; transformed into digital form, enabling both digital and analogue presentation of information; allows user interactivity through computer interface interaction with the presentation's narrative.

Particularly for multimedia works, Section 12a of the Audiovision Act is crucial as it allows for the use of other recognised labelling systems besides the unified system established by this law. According to Decree No. 78/2023 Coll. by the Ministry of Culture of the Slovak Republic on accepted labelling systems, one such system is the Pan European Game Information (PEGI), which also establishes that the age suitability and type of potentially harmful content of a multimedia work can be determined according to the PEGI content rating system in accordance with the PEGI Code of Conduct. PEGI is a European content rating system for electronic games developed by the Interactive Software Federation of Europe, used since 2003.

The Audiovision Act establishes a specific unified labelling system, which is mandatory for classifying audiovisual works, multimedia works, television programme services, and on-demand audiovisual media services, collectively referred to by the law as a “communication”. This system is designed to protect minors and consists of labelling these communications by: age suitability for age groups under 7, 12, 15, or 18 years in terms of their appropriateness or inappropriateness; descriptors regarding the presence of potentially harmful content contained within them.

The unified labelling system and details of its implementation are specified in a general binding regulation issued by the Ministry of Culture of the Slovak Republic upon the proposal of the Commission for the Protection of Minors. Section 12 of the Audiovision Act specifies that this generally binding legal regulation must establish: assessment criteria for inaccessibility or inappropriateness, which must be used when evaluating content for the protection of minors, particularly the present level of physical, psychological, or verbal violence, depicted sexual relationships or scenes, nudity in a sexual context, vulgar language, depiction of drug use, gambling or other dependencies, as well as the presence of depictions or other manifestations causing feelings of fear, depression, helplessness, or otherwise inappropriate in relation to a

specific age group of minors; assessment criteria for suitability in relation to a specific age group of minors for whom the content is recommended; methods of marking the communication with age suitability in terms of its inappropriateness or appropriateness; assessment criteria that must be considered when evaluating the content of the marked communication in terms of the presence of potentially harmful content types, especially those depicting violence, sex, fear, discrimination, dependency, or vulgar language; methods of marking the communication in terms of the presence of potentially harmful content; details on the application of obligations by persons required to apply the unified labelling system in evaluating content, its categorisation according to age suitability and type of potentially harmful content, labelling, and public presentation; details on the application of obligations established by the Media Services Act.

The Ministry of Culture of the Slovak Republic issued Decree No. 328/2023 Coll. on the Unified Labelling System and the Method of Its Application (hereinafter, “Decree on the Unified System”), which specifies the legal obligations of the unified labelling system designed to protect minors. This Decree classifies various types of potentially harmful content for minors, considering different age categories of minors. It establishes categories for minors under 18, 15, 12, and 7 years, providing the most detailed legal regulation that distinguishes between minors and the legal protection provided to them in the media and digital spaces. According to the Decree on the Unified System, individual audiovisual works, multimedia works, television programming services, and on-demand audiovisual media services, henceforth referred to as “communications”, can be classified with a descriptor that refers to a specific type of potentially harmful content. The descriptors used to label the communications specifically indicate threats to minors from factors such as i) violence, ii) discrimination, iii) fear, iv) dependency, v) sex and nudity, vi) vulgar language. The labelling of communications under this Decree is carried out using a content descriptor that includes a specific letter indicating the presence of content that poses a risk to young individuals, as well as pictograms of the content descriptor, which are distinctively colour-coded. It is stipulated that a television programming service classified as inappropriate for minors under 18 years may only be broadcast between 10:00 PM and 6:00 AM. One classified as inappropriate for minors under 15 years may be broadcast between 8:00 PM and 6:00 AM. Furthermore, the Decree on the Unified System regulates that before, during, and after broadcasting a programme classified as inappropriate for minors under 7 years, or conversely appropriate for minors under 12 years, a programme classified as inappropriate for minors under 15 years or as inappropriate for minors under 18 years cannot be scheduled.

This comprehensive regulatory approach, as stipulated by the Decree on the Unified System, ensures that the content available to minors in Slovakia is monitored and controlled to prevent exposure to inappropriate material, effectively safeguarding their development and well-being in the media landscape. This method of strict scheduling and content classification seeks to balance the availability of diverse

content with the need to protect younger viewers from content that could negatively influence their psychological or moral development.

In the Slovak regulatory framework, the content of communications and media is meticulously classified to protect minors from exposure to potentially harmful materials. The categories set forth by the legislation are designed to ensure that media content adheres to age-appropriate guidelines, recognising the developmental needs and sensitivities of different age groups. Here is an overview of how certain types of content are classified according to the suitability for minors:

Content is classified as inappropriate for minors under 18 if it depicts: violence on human beings that involves cruel injury or cruel violent death without a sense of remorse, or torture of a person, or violence using weapons as a means of assault for entertainment purposes; displays of discrimination, intolerance, or hatred linked with violence or other inappropriate behaviours, if such behaviours are endorsed; displays of pathological behaviour intentionally inducing fear or anxiety; depictions or presentations of the use of narcotics or psychotropic substances, gambling, or other behaviours that could lead to substance or non-substance addiction, if portrayed as entertainment and endorsed, despite such behaviours being socially unacceptable; pornography; sexual scenes or sexual behaviours including promiscuous behaviour, presented as a form of entertainment; sexual scenes associated with expressions of sexual violence or sexual deviance; vulgar expressions, vulgar gestures, obscene expressions, or obscene gestures, where owing to their contextual occurrence, frequency, processing method or depiction, and considering the character, type, and artistic and moral message of the work or programme, they are deemed appropriate only for persons aged 18 and over.

Content is classified as inappropriate for minors under 15 if it contains: detailed and naturalistic violent acts; animal abuse; the use of weapons as a means of assault, where the depiction inappropriately endorses, trivialises, or excessively exploits the use of weapons; displays of discrimination, intolerance, or hatred, if such behaviours are trivialised or highlighted as valuable and commendable; situations inducing feelings of fear or anxiety; behaviours with a high risk of harm to human health presented as attractive or entertaining, without warning of its dangers or presented without impending harmful consequences; depictions or presentations of alcoholism, smoking, consumption of narcotics and psychotropic substances, gambling, or other behaviours that could lead to substance or non-substance addiction, where any form of addiction is endorsed, trivialised, or highlighted as valuable; explicitly depicted sexual scenes that are part of the storyline; expressive or vulgar expressions, vulgar gestures, obscene expressions, or obscene gestures, where owing to their contextual occurrence, frequency, processing method or depiction, and considering the character, type, and artistic and moral message of the work or programme, they are deemed appropriate only for minors aged 15 and over.

Content is classified as inappropriate for minors under 12 years old if it includes: real violence or depiction of the consequences of real violence on a living being, the aftermath of natural disasters, armed conflicts, or traffic accidents; psychological

violence, especially verbal abuse, or instructions for psychological harm; violent acts or depictions of the consequences of violent acts; blood and bodily disfigurement that are not common in nature; behaviour with a risk of injury if the risk is not clearly communicated; risky sports disciplines or situations where an inadequate interpretation relative to age might lead to imitation by minors; depiction of a sexual scene without nudity or sexual behaviour that is part of the storyline; expressive language that, given its contextual occurrence, frequency, and the manner and form of its presentation, as well as considering the character, type, and artistic and moral message of the work or programme, is deemed appropriate for minors from 12 years old; depiction of nudity that is not usual in normal family settings or public places.

Content is classified as inappropriate for minors under 7 years old if it contains: forced violence on helpless beings, especially on children or animals; aggressively attacking living beings or objects that induce fear; depiction of environments in dark and gloomy colours, or scenes with overly loud music or abrupt audio or visual changes; threats to family relationships or the endorsement of dysfunctional interpersonal relationships; depiction of a negative storyline involving a child that could cause a child to experience real-world victim effects; depiction of behaviour with a risk of injury, if the risk is not clearly communicated, or depiction of fantastical ideas about superhuman heroic acts that are outside the real world, where an inadequate interpretation relative to age might lead to imitation by minors.

The protection of minors in accordance with the provisions of the Audiovision Act is particularly secured through the establishment of a commission as a special co-regulation body for the area of minor protection when applying the unified labelling system or another accepted labelling system, such as the previously mentioned PEGI system used for multimedia works. The commission's responsibilities include drafting proposals for general binding legal regulations that establish details about the unified labelling system and the method of its application, which are submitted to the Ministry of Culture of the Slovak Republic, supervising compliance with obligations under the Audiovision Act and the Media Services Act, as well as providing methodical guidance on procedures for determining age suitability by individuals conducting age suitability assessments.

The National Concept of Child Protection in the Digital Realm not only delineates the digital space as encompassing information and communication technologies – including the Internet, mobile and associated technologies and devices, as well as digital networks, databases, contents, and services – but also references additional threats faced by minors in relation to their participation in the digital environment. This Concept highlights terms such as cyberbullying, grooming (characterised by relationship and trust building between a sexual predator and victim, often through the creation of a false digital identity), happy slapping (a form of bullying involving recording an attack on an unsuspecting victim and disseminating the footage via mobile or Internet to ridicule the victim), sexting (the sending of messages, photos, or videos with erotic and sexual content through information and communication technologies), and webcam trolling (a fraud where the perpetrator uses a prerecorded

video, perceived by the victim as a live webcam image, to deceive and extract sensitive data, including nude photos or videos from the victim).¹² Furthermore, the National Concept identifies a significant issue in that the legal regulations of the Slovak Republic do not clearly define how to approach cases of minor abuse in the digital realm.

This conclusion can be agreed with; however, we believe that even under the current state of the law (*de lege lata*), the legal framework provides basic legal remedies for the protection against such abuse of minors. Regarding the creation and potential use of image and sound recordings concerning an individual, such actions may only occur with the person's consent or under what are termed statutory licences. Otherwise, it constitutes an unauthorised intrusion into the personality rights of an individual, warranting consideration of the application of personal rights protections under Sections 11 to 16 of the Civil Code for minors. Exceptions to the principle that the creation and use of personal expressions are only possible with the consent of the affected person are outlined in Section 12 (2 and 3) of the Civil Code, which regulates so-called statutory licences.¹³

Moreover, the National Concept correctly indicates that the actions could fulfil the elements of certain criminal offences anticipated by Act No. 300/2005 Coll., the Criminal Code, as amended.

The Criminal Code, in Section 132, provides legal definitions of notions of pornography and child pornography. Pornography, for the purposes of the Criminal Code, is defined as the depiction of intercourse, other forms of sexual intercourse or similar sexual contact, or the depiction of exposed genital organs intended for sexual purposes. Child pornography is defined as the depiction of actual or simulated intercourse, other forms of sexual intercourse or similar sexual contact with a child or a person appearing to be a child, or the depiction of exposed body parts of a child or person appearing to be a child intended for sexual purposes. A child pornographic performance is a live performance intended for an audience, even using information technology, in which a child is involved in actual or simulated sexual conduct, or in which parts of a child's body intended for sexual purposes are exposed. For the purposes of the Criminal Code, a child is considered a person under 18 years.

The Criminal Code further specifies several provisions that define crimes related to minors, which can also occur within the digital space. Notably, the crime of disseminating child pornography, committed by reproducing, making available, or otherwise disseminating such material, often occurs within the digital realm. Additionally, the crime of possessing child pornography and participating in a child pornographic performance involves actions intentionally aimed at gaining access to child pornography through an electronic communication service. The offence of endangering morals can also occur by offering pornography to a child or at a place accessible to children. Regarding the endangerment of minors in the digital space, it is also worth noting the crime of dangerous stalking, according to Section 360a(1)(c)

12 Bacigál et al., 2020, pp. 2–3.

13 Vozár, 2019, p. 81.

of the Criminal Code, committed by anyone who persistently pursues another in such a way that may reasonably cause fear for their life or health or that of someone close to them, or substantially worsens their quality of life, by contacting them through an electronic communication service, in writing or otherwise against their will. However, we consider it essential to point out that contact must always occur against the will of the harmed party. It is not enough that the contact is simply unpleasant for the harmed party; the harmed party must clearly express opposition to the contact, and the perpetrator must be aware of this.¹⁴

The Criminal Code also defines the crime of dangerous electronic harassment, which, while not exclusively protecting only minors, provides them protection by deeming such conduct criminal. The described criminal offence was incorporated into the Criminal Code only by the 2021 amendment. We believe that this legal change represents a qualitatively significant positive shift, as it responds to the real need for prosecuting a specific unlawful act that perpetrators are increasingly committing in the digital environment. Unfortunately, the victims of such acts are often minors. This offence, according to Section 360b of the Criminal Code, is committed by anyone who, intentionally via an electronic communication service, computer system, or network, substantially worsens another person's quality of life by: persistently humiliating, intimidating, acting unauthorisedly on their behalf, and persistently harassing them, or unlawfully publishing or making accessible to a third party any visual, auditory, or audiovisual recording of their personal expression obtained with their consent, capable of significantly endangering their dignity or causing other serious harm to their rights.

Based on the National Concept of Child Protection in the Digital Space, as well as the prevailing and effective legal framework in the Slovak Republic, it can be summarised that the following entities primarily participate in ensuring institutional and policy support for the protection of children in the digital environment: the Office of the Government of the Slovak Republic; the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatisation; the Ministry of the Interior of the Slovak Republic and the Government Council for Crime Prevention; the Ministry of Culture of the Slovak Republic; the Ministry of Justice of the Slovak Republic; the Office of the Commissioner for Children; the Office for Personal Data Protection of the Slovak Republic; the Police Force, prosecution, and courts of the Slovak Republic; the Council for Media Services.

In connection with this topic, the project *Zodpoved.sk*, which operates as the national centre for safe Internet under the civil association *eSlovensko o. z.*, should not be overlooked. This project is funded by the European Union under the Safer Internet community programme. Its partners have included the Ministry of the Interior of the Slovak Republic, the Ministry of Education, Science, Research and Sport of the Slovak Republic, and the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatisation. The main objectives of the project

14 Burda et al., 2011, p. 1130.

include: management and operation of the national awareness centre [Zodpovedne.sk](https://www.zodpovedne.sk); increasing awareness and spreading education about responsible internet use, mobile communication and new technologies, and crime prevention; ensuring and operating the help line [Pomoc.sk](https://www.pomoc.sk); engagement in international networks, sharing experiences of other national centres and organisations for information technology security; establishment and operation of the national centre for reporting illegal content and activities on the Internet, [Stopline.sk](https://www.stopline.sk).¹⁵

Following the Act on the Commissioner for Children, the Office of the Commissioner for Children was established in the Slovak Republic, which contributes to the support and enforcement of children's rights. Under this law, the Commissioner for Children operates in Slovakia, particularly assessing the observance of children's rights, both as an official duty and based on individual complaints. For this purpose, the Commissioner monitors compliance with the rights of the child, especially by conducting independent investigations to fulfil obligations arising from international treaties to which Slovakia is bound, performing systematic visits to special educational institutions and facilities for social and legal protection of children and social guardianship, and other places where children may be restricted in their freedom by public authorities. The Commissioner also collaborates directly with children or through organisations active in the field of children's rights. Among the special powers of the Commissioner is the right to speak with a child, who is placed in detention, serving a sentence, under protective treatment or educational measures, or in institutional care, without the presence of third parties. The Commissioner has a special right to participate in court proceedings. The Commissioner for Children submits an annual report on his activities to the National Council of the Slovak Republic, in which he also evaluates the state of child rights protection in Slovakia.

2. The Right to Privacy and the Right to be Forgotten

The right to erasure of personal data is legislated under the Personal Data Protection Act. Essentially, this right builds upon the general legal framework for the protection of personality as outlined in the Civil Code, wherein privacy is specifically safeguarded for every individual, including minors, against unauthorised intrusions. Such unauthorised intrusions include the unlawful collection of personal data about an individual, or the subsequent retention of such data despite the individual's objection and the absence of any legal basis permitting such retention without the consent of the concerned individual.¹⁶

Building on this principle, the Personal Data Protection Act imposes an obligation, under legally specified conditions, on data controllers – who are defined in Section

15 For further reference, see: <https://www.zodpovedne.sk/index.php/sk/kontakt> (Accessed: 18 February 2025).

16 See: Vojčík et al., 2021, p. 141.

5(o) of the Act as anyone who alone or jointly with others determines the purposes and means of the processing of personal data and processes personal data in their own name – to erase personal data without undue delay. Data must be erased if one of the following conditions is met: the personal data are no longer necessary for the purpose for which they were collected or otherwise processed; consent by the data subject for the processing of their personal data has been withdrawn, and there is no other legal ground for processing; the data subject objects to the processing of their personal data carried out to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, and there are no overriding legitimate grounds for the processing; the processing of the personal data is unlawful; the personal data must be erased to comply with a legal obligation; the personal data were collected in relation to the offer of information society services.

The definition of information society services is further specified in another piece of legislation, namely, the Electronic Commerce Act (Act No. 22/2004 Coll., as amended), which stipulates that an information society service is a service provided remotely by electronic means at the individual request of a recipient of services, usually for a fee. This encompasses commercial communication, processing, transmission, storage, retrieval, or collection of data and electronic mail except for personal electronic mail. It is also specifically stated that information society services do not include broadcasting and television broadcasting, including teletext, voice telephony services, fax services, and services whose content precludes their provision at a distance.

Regarding the protection of minors, the Personal Data Protection Act specifically considers this group by setting a special age threshold of 16 years, which upon reaching, a minor may independently consent to the processing of personal data related to the offer of information society services. If the individual is under 16 years old, such processing of personal data is lawful only if and to the extent that such consent has been given or authorised by the minor's legal guardian. The law specifically requires that the controller must make reasonable efforts to ensure that the legal guardian has provided or approved the consent for processing the personal data, considering available technology.

3. Freedom of Expression and the Right to Information

The Constitution of the Slovak Republic, in Article 26, guarantees every individual the right to information and freedom of expression. These are fundamental human rights, categorised as political rights. The essence of freedom of expression includes the right to freely express one's opinions in any form, be it verbally, in writing, through print, visually, or through any other means that may be considered appropriate given the advancements and current state of technology. The Constitution of the Slovak Republic also recognises the right of every individual to freely seek, receive, and disseminate ideas and information without regard to state borders, while

ensorship is prohibited. As is the case with other fundamental rights and freedoms, the Constitution of the Slovak Republic stipulates and expressly provides that the freedom of expression, as well as the right to seek and disseminate information, may be restricted by law. However, such restrictions must consist of measures prescribed by law that are necessary in a democratic society for the protection of the rights and freedoms of others, for state security, public order, or the protection of public health and morals. Specifically, the protection of the morality of minors is an objective targeted by legal regulations limiting access to certain broadcast programmes, which was the subject of analysis in the previous section of the text. Such constitutionally anticipated restrictions may occur, for example, under Act No. 69/2018 Coll., on Cyber Security and on amendments to certain laws, as amended, according to which the National Security Authority has the authority to decide on blocking harmful content or activities directed into or from the cyberspace of the Slovak Republic.

In addition to the above, freedom of expression is also limited by the fundamental rights and freedoms of other individuals.¹⁷ The Internet has not only changed the factual way of communication and expression but has also brought changes in the legal understanding of freedom of expression.¹⁸ Public forums, such as blogs, social networks, discussion rooms, and websites, have led to an increase in controversial expressions, primarily due to the lack of communication regulation in virtual space.¹⁹

For this reason, we believe it is essential for the judiciary to reflect these realities and that the decisions must clearly outline the legal limits of freedom of expression, particularly in digital space, especially when directed at a minor recipient. The fact that the right to freedom of expression is not an absolute right, and in certain situations must yield, was confirmed by the Constitutional Court of the Slovak Republic in its Resolution II. ÚS 78/2019 dated 23 May 2019.

In this context, we also refer to the Constitutional Court's ruling III. ÚS 110/2020 dated 24 April 2019, in which the court pointed out that the absolute restriction of freedom of expression in that case was contrary to the law because there was no urgent social need for it. The privacy of the minor could have been effectively protected through other, less intrusive means, such as ensuring her anonymity in the relevant article or prohibiting the publication of her photograph. From this, it follows that disproportionate interference with the rights of others cannot occur and must not be overlooked even in the interest of protecting minors.

17 See: Záhora, 2024, p. 389.

18 Strážnická, 2018, p. 116.

19 Antić, 2023, p. 74.

4. Freedom of Expression and the Right to Be Heard

The right to freedom of expression is closely linked with the right to be heard, which in the case of minors can be directly derived from the Family Act. Article 5 of the basic principles of this Act emphasises that the paramount consideration in decisions involving matters concerning a minor is in the child's best interest. Among other factors, this interest must consider the minor's own opinion, which is reflected not only in substantive law but also in procedural law. Act No. 161/2015 Coll., on Civil Non-Contentious Proceedings, as amended, which governs proceedings concerning minors, specifically states that if a minor capable of independently expressing their opinion is a party, the court must consider this opinion before evaluating what is in their best interest.

This fact is repeatedly confirmed in the case law of the courts of the Slovak Republic. We refer to the Resolution of the Constitutional Court of the Slovak Republic, case no. II. ÚS 56/2017, dated 19 January 2017, in which the court stated that in order to achieve a just decision on the regulation of contact between parents and their minor child, the court must take into account the wishes of the minor child among other things.

The method of ascertaining the opinion of the minor must be appropriate to their age and maturity and may occur without the presence of other individuals. It is noted that for the purposes of civil proceedings, a minor is defined as any person under the age of 18 years. However, the right to be heard for minors is realised not only in civil proceedings during judicial decision-making but also, for example, in the provision of healthcare, where, except in certain situations, the informed consent of the patient is always required. This consideration ensures that the minor's views are considered in contexts that significantly affect their lives, thereby reinforcing the principle that their views matter in decisions that concern them. In the case wherein the patient is a minor child, the legal framework of Act No. 576/2004 Coll. on Healthcare, Services Related to Healthcare Provision, and Amendments and Supplements to Certain Laws, as amended (hereinafter, "Healthcare Act"), grants the right to be informed and to give subsequent informed consent on behalf of the minor child to their legal representative or to the person who provides substitute personal care for the minor child, or who is their guardian or custodial guardian.²⁰

Simultaneously, however, the legal framework requires that when making decisions, the minor patient should participate to the greatest extent possible, and their opinion must be considered.

20 Humeník, 2011, p. 69.

5. The Right to Education and the Right to Information

The Constitution of the Slovak Republic guarantees the right of education to everyone without discrimination, and school attendance is mandatory until the age limit established by law, which is currently 16 years. This means that compulsory education lasts until the end of the school year in which the student turns 16, with the expected duration of compulsory schooling being 10 years. The Constitution also considers citizens belonging to national minorities or ethnic groups, guaranteeing under conditions specified by special laws, the right to education in their language. The right to education entails the duty of minors to cooperate with their parents, enabling them to carry out the care and upbringing of the children. Concurrently, minors have the obligation to fulfil their educational responsibilities commensurate with their abilities.

The Constitutional Court of the Slovak Republic has also commented on the essence of the basic right to education. In its Ruling No. PL. ÚS 11/2013 dated 22 October 2014, the court stated the following:

‘The essence (core) of the basic right to education is the right to access to education. Therefore, in principle, all legally established interventions aimed at limiting access to education raise constitutional concerns and require careful consideration. The right to education, with its key component being the right to access education, is not an absolute right, i.e., the legislator may limit it, but only under the condition that such limitations respect its essence and purpose, and are used only for an established (legitimate) goal (Article 13, Paragraph 4 of the Constitution of the Slovak Republic). The legally established average grade during primary school as a criterion for selecting students applying for study at a secondary vocational school with a high school diploma or at a gymnasium has indisputable relevance, especially because it can serve as a motivational factor for the affected group of students. In the challenged legal regulation, the criterion of not achieving the legally established average grade has a disqualifying character, i.e., it automatically prevents students from accessing studies at gymnasiums and secondary vocational schools with a high school diploma. Under these circumstances, the mentioned criterion, and thus the challenged legal regulation, could withstand constitutional scrutiny only if it were sufficiently objective and excluded clearly unjustified interventions into the right to access complete secondary education.’

In the context outlined above, an important earlier ruling is also the Resolution of the Constitutional Court of the Slovak Republic, case No. II. ÚS 37/94, dated 7 September 1994, in which the court stated that according to Article 42, Paragraph 2 of the Constitution of the Slovak Republic, citizens have the right to education according to their abilities and the possibilities of society, including at universities. Therefore, if the abilities of an applicant for university studies are evaluated in the same legal

manner as those of other applicants, a decision by the dean of the faculty regarding the rejection of an applicant for studies cannot constitute a violation of their rights.

In the context of the digitisation of public environments, it is imperative to consider these aspects in securing children's right to education. Recognising this, Slovakia has enacted laws providing support to citizens during their studies. The Ministry of Investments, Regional Development, and Informatisation of Slovakia, in cooperation with the Digital Coalition- National Coalition for Digital Skills and Professions SR, launched in 2023 the national project "Digital Grant for Pupils of Slovakia (Digital Student)",²¹ which provided selected groups of students with a one-time grant of EUR 350 to purchase a laptop or tablet with a keyboard. The grant aimed to assist students from elementary and secondary schools coming from socially weaker environments, who otherwise lacked access to the devices necessary to take advantage of the benefits associated with digital space. Access to devices that connect to the Internet also ensures access to information, predominantly disseminated and accessible online in the digital era.

6. Summary

Following the adoption of the National Concept for the Protection of Children in the Digital Space, and particularly through the subsequent enactment of the Media Services Act and the Audiovisual Act, Slovakia now possesses a fundamental legal framework regulating the rights and obligations of media content distributors not only offline but also online, thereby ensuring special protection for minors. Slovakia, based on the current wording of its legal regulations, respects the Directive of the European Parliament and of the Council (EU) 2018/1808 of 14 November 2018, which amended the Directive on Audiovisual Media Services. However, the legal protection of minors in the digital space is not only ensured by the requirement for broadcasters or providers of video-sharing platforms to label content that is inappropriate for minors. Their protection is also secured through the Personal Data Protection Act, which includes, among other provisions, the right to be forgotten. Moreover, various public projects institutionally secured by the state in cooperation with the third sector provide education to minors about the dangers associated with using the Internet. Finally, the protection of minors is also ensured by criminal law standards, the application of which, however, is contingent upon meeting the elements of specific criminal offences.

21 For further reference see: <https://digitalnyziak.sk> (Accessed: 18 February 2025).

Bibliography

- Antić, P. (2023) 'Sanctioning Hate Speech on the Internet: In Search of the Best Approach', *Pravni Zapisi: časopis Pravnog Fakulteta Univerziteta Union u Beogradu*, 14(1), pp. 74–100; <https://doi.org/10.5937/pravzap1-43118>.
- Bacigál, I., et al. (2020) 'Národná koncepcia ochrany detí v digitálnom priestore' [Online]. Available at: https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf (Accessed: 16 January 2025).
- Burda, E., et al. (2011) *Trestný zákon*. Kommentar II. Praha: C.H. Beck.
- Drgonec, J. (2019) *Ústava Slovenskej republiky*. 2nd edn. Bratislava: C.H. Beck.
- Funta, R. (2020) 'Fúzie a ich vplyv na osobné údaje spotrebiteľov v dimenziách práva Európskej únie', *Justičná revue*, 72(3), pp. 307–335.
- Funta, R., Horváth, M. (2024) 'Uplatňovanie GDPR ako prostriedok monopolizácie trhu?', *Justičná revue*, 76(3), pp. 281–294.
- Humeník, I. (2011) *Ochrana osobnosti a medicínske právo*. 1st edn. Bratislava: EUROKÓDEX.
- Kalesná, K., Patakyová, M.T. (2021) 'Digitálne platformy: súťažné právo verzus regulácia ex ante', *Právny obzor*, 104(1), pp. 26–38; <https://doi.org/10.31577/pravnyobzor.2021.1.02>.
- Kasenčáková, L. (2016) 'Internet ako priestor porušovania pravidiel hospodárskej súťaže' in Lenhart, M., et al. (eds.) *Zborník príspevkov z konferencie Bratislavské právnické fórum 2016*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, pp. 58–68.
- Mičudová, T. (2023) 'Zákon o mediálnych službách', *Práca, mzdy a odmeňovanie*, 2023/8, pp. 44–45.
- Strážnická, A. (2018) 'Sloboda prejavu na internete' in Andraško, J., Hamulák, J. (eds.) *Bratislavské právnické fórum 2018: ústava na internete a internet v ústave*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta UK, pp. 116–123.
- Števček, M.A. et al. (2019) *Občiansky zákonník I. § 1–450*. Komentár. 2nd edn. Praha: C.H. Beck.
- Vojčík, P., et al. (2021) *Občianske právo hmotné*. Vol. 1. 3rd edn. Plzeň: Aleš Čeněk.
- Záhora, J. (2024) 'Sloboda prejavu vs. nenávisťné prejavy na internete', *Právny obzor*, 107(4), pp. 384–407; <https://doi.org/10.31577/pravnyobzor.2024.4.03>.

Children in Digital Age – Slovenian Perspective

Benjamin LESJAK

ABSTRACT

This country report explores the use and impact of digital devices among Slovenian children and adolescents, along with the Slovenian legal framework concerning children's rights, specifically in the context of digital services and social media. It reveals that smartphones are the most used devices among Slovenian youth, with significant hours spent on them daily. Television and computers are also commonly used, though less so than smartphones. The influence of parents in guiding technology use and the popularity of various social networks among different age groups are highlighted. Legal definitions of a child and minor, as well as the role of parents, are explored within the Slovenian legal system. The document further examines Slovenia's stance on children's rights in the digital era, emphasising the lack of a specific law for children's rights while acknowledging the Constitution and Family Code's role in ensuring their protection. The role of public institutions, legal remedies, and education in safeguarding children in the digital space is also examined, highlighting the contributions of various organisations and legal acts in promoting safe internet use and protecting children's rights online. The abstract underscores the complexity and evolving nature of children's digital rights, emphasising the need for continued vigilance and adaptation to protect these vulnerable members of society.

KEYWORDS

digital device usage, Slovenian adolescents, legal framework, children's rights, online content regulation

1. Definitions and Taxanomic Rationale

1.1. Statistics

When discussing the use of digital devices among children or adolescents in the Slovenian context, three devices take the lead: smartphones, television, and computers. Children aged 12 to 15, or primary school students, use these devices on average one to three hours per day, with a quarter using smartphones more frequently – specifically three to five hours daily – and a fifth using them for over five hours daily. Among individuals aged 15 to 19, or high school students, smartphone usage is even higher, with most using them for three to five hours daily and a significant quarter using

Benjamin LESJAK (2025) 'Children in Digital Age – Slovenian Perspective' in Halász, Cs. (ed.) *Children in Digital Age*. Miskolc-Budapest: Central European Academic Publishing, pp. 265–290.
https://doi.org/10.71009/2025.csh.cida_13.



them for five to ten hours daily. The second most common device that adolescents use is television, as they watch it for approximately one to three hours per day, with high school students spending significantly more time watching streaming TV content than primary school students. Adolescents use computers on average for one to three hours per day, and slightly less than half use them for less than an hour per day. Among Slovenian adolescents, the radio is the least frequently used medium. Most of them have never used virtual reality glasses, and just under half have used gaming consoles (such as PlayStation) or tablets. Most adolescents, both primary and high school students, use digital devices during rest and relaxation, simultaneously while watching television, and before bedtime. Primary school students use devices the least during reading, while high school students use them during lunch or dinner. The habits of adolescents are significantly influenced by their parents. Parents guide the use of technologies by adolescents, most commonly warning them about the dangers of devices, though they less frequently prohibit specific content. The use of devices is employed as a means of discipline, mainly when adolescents violate family rules or receive poor grades. Almost half of primary school students' parents also follow them on social networks and check their activities on devices.¹

Among the content or accompanying media that adolescents follow on devices, personalised music apps are the most popular, with almost two-thirds of primary school students using them daily. Streaming TV content comes in second place, with about a third of them using it daily, while podcasts and online newspapers are not as popular. Online platforms or social networks are the most used platforms among adolescents, with almost all of them using them – 96% of primary school students and 98% of high school students. Preferred social networks among Slovenian adolescents include Snapchat, TikTok, YouTube, and Instagram, with Discord and Pinterest also being common choices. Only a few per cent of adolescents use Facebook. Among primary school students, Snapchat is the most popular, while Instagram is the favourite among high school students. Most adolescents use their phones, apps, and social networks primarily for daily conversations, listening to music, or sending private messages; they post their own content the least.²

1.2. Definitions

The Family Code³ defines a child as a person who has not yet reached the age of 18, unless they have acquired full legal capacity before that. The Family Code replaced the Marriage and Family Relations Act,⁴ which did not contain a definition of a child.

1 Črnič et al., 2023, pp. 12–25.

2 Ibid., pp. 26–36.

3 Family Code, Uradni list RS, št. 15/17, 21/18 – ZNorg, 22/19, 67/19 – ZMatR-C, 200/20 – ZOOMTVI, 94/22 – odl. US, 94/22 – odl. US in 5/23.

4 Marriage and Family Relations Act, Uradni list RS, št. 69/04 – uradno prečiščeno besedilo, 101/07 – odl. US, 90/11 – odl. US, 84/12 – odl. US, 82/15 – odl. US, 15/17 – DZ in 30/18 – ZSVI.

In accordance with Article 8 of the Constitution of the Republic of Slovenia⁵ (hereinafter: the Constitution), which establishes the direct application of ratified and published international treaties, the definition of a child as per the Convention on the Rights of the Child⁶ was applied as the law applicable to the child specifies an earlier age of majority. Despite the direct application of the Convention on the Rights of the Child, Article 5 of the Family Code expressly stipulates that a child is a person who has not yet reached the age of 18. The onset of adulthood at the age of 18 is an objective criterion that distinguishes a child from an adult. With the commencement of the child's chronological eighteenth year, a legal presumption arises, based on which it is presumed that the child is sufficiently old and mature to acquire full legal capacity. The Family Code also specifies exceptions to this presumption. Childhood can be terminated in advance by judicial emancipation of the child, by acquiring full legal capacity, specifically in the case of the child entering into marriage or becoming a parent. In the Republic of Slovenia (hereinafter: Slovenia), a child under the age of 18 requires representation by a legal representative, who can be a parent or guardian, for the performance of procedural acts and the conclusion of legal transactions, with the exception of family law disputes, where full procedural capacity is recognised at the age of 15.⁷ In criminal proceedings, a minor who has reached the age of 16 can independently submit a proposal or file a private lawsuit.⁸

The concept of a minor is not specifically defined in Slovenian legislation. Generally, it is understood to refer to a person under the age of 18.⁹ According to the stance of the Second Instance Court, in Slovenian legislation, terms such as “child”, “minor person”, “minor blood relative”, “minor”, “person under the age of 15”, and “minor victim” are used for these individuals. This is particularly evident in the twenty-first chapter of the Criminal Code,¹⁰ where the term “child” is used in the title, while various terms are used in specific articles.¹¹

Similarly, in the Slovenian legal system, there is no specific legal definition of the term parents. In accordance with the provisions of the Family Code, it can be inferred that parents are the bearers of rights and obligations. To the best of their abilities they are tasked with creating conditions that ensure the comprehensive development of the child, known as parental care. Parental care is a joint responsibility of both parents and ceases when the child reaches the age of 18 or if the child acquires full

5 Constitution of the Republic of Slovenia, Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121, 140, 143, 47/13 – UZ148, 47/13 – UZ90, 97, 99, 75/16 – UZ70a in 92/21 – UZ62a.

6 Convention on the Rights of the Child, adopted by the United Nations General Assembly through Resolution 44/25 on 20 November 1989.

7 Kraljič, 2019, pp. 61–63.

8 Article 54 para. 2 of the Criminal Procedure Act, Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP in 16/23).

9 Article 24 of the Family Code.

10 Criminal Code, Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP in 16/23.

11 Ljubljana Higher Court, Sodba V Kp 48/2010 dated 11 November 2010.

legal capacity before reaching majority.¹² With the cessation of parental care, parents are no longer the child's legal representatives. At that point, the child achieves legal emancipation from the parents. The constitutional basis for the institute of parental care is provided by Article 54 of the Constitution, which grants parents the right to educate and raise their children. Parents, in exercising parental care, are unlimited in relation to others unless their parental care is restricted or revoked. However, the best interests of the child restrict their actions. The fundamental guiding principle for parents in caring for the child is, indeed, the best interests of the child. Parental care initially belongs to both parents, but the court can prohibit one of them from exercising certain rights in cases where the child's well-being is endangered.¹³

The Slovenian legislator defines the concept of digital services in the Consumer Protection Act.¹⁴ It is characterised as a service that enables consumers to create, process, or store data in digital form or to access such data. Additionally, it includes services that facilitate the exchange of data in digital form or any other form of interaction with this data, uploaded or generated by consumers or other users of the service.¹⁵ It is essential to distinguish the concept of digital services from the term "information society service", which, in accordance with the Electronic Commerce Market Act,¹⁶ represents a service typically provided for remuneration, remotely, using electronic means, and at the individual request of the service recipient.¹⁷

Slovenian legislation also does not provide a definition for social media. In the year of 2017, the court interpreted social media as a means of public communication with an indefinite circle of individuals and falls within the realm of the World Wide Web (Internet).¹⁸

1.3. Legal Framework

The position and rights of children in Slovenia are among the priority objectives of Slovenian foreign policy. Slovenia is also recognised for its role in numerous international initiatives, including advocating for the inclusion of human rights education on the agenda of the United Nations and addressing the issue of children in armed conflicts within NATO.¹⁹ In 1992, Slovenia inherited the United Nations Convention on the Rights of the Child from its predecessor, the Socialist Federal Republic of Yugoslavia. This inheritance occurred through the Fundamental Constitutional Charter on the Independence and Sovereignty of the Republic of Slovenia²⁰ and the Notifi-

12 Art. 6 and Art. 152 para. 2 of the Family Code.

13 Kraljič, 2019, pp. 62–68.

14 Consumer Protection Act, Uradni list RS, št. 130/22.

15 Art. 4 para. 3 of the Consumer Protection Act.

16 Electronic Commerce Market Act, Uradni list RS, št. 96/09 – uradno prečiščeno besedilo, 19/15, 189/21 – ZDU-1M in 18/23 – ZDU-10.

17 Art. 3 para. 11 of the Electronic Commerce Market Act.

18 Maribor Higher Court, Sklep I Kr 32384/2017 dated 14 November 2017.

19 Erjave, 2014, p. 5.

20 Fundamental Constitutional Charter on the Independence and Sovereignty of the Republic of Slovenia, Uradni list RS, št. 1/91-I in 19/91 – popr.

cation of Succession regarding conventions of the United Nations.²¹ By supporting various projects aimed at improving the well-being of children, Slovenia has gained a reputation as an advocate for children's rights at the international level since gaining independence in 1991.²² In 1999, Slovenia also ratified the European Convention on the Exercise of Children's Rights.²³

The rights of children in Slovenia are subject to the protection of conventions, and there is no specific law that regulates children's rights. As the fundamental and highest general legal act of Slovenia, the Constitution, in Article 56, stipulates that children are entitled to special protection and care, and they enjoy human rights and fundamental freedoms in accordance with their age and maturity. Children are provided with special protection against economic, social, physical, mental, or other exploitation and abuse. The law also specifically regulates the position of children and minors whose parents do not care for them, who have no parents, or lack appropriate family care, and enjoy special protection from the state. The Constitution mandates compulsory primary education financed from public funds, and the state creates opportunities for citizens to acquire proper education.²⁴ Compulsory primary education, in keeping with the Basic School Act,²⁵ is organised as a unified nine-year primary school for children between six and 15 years old. The Family Code, as a crucial legal framework for regulating family relationships and the rights of children, adheres to the fundamental principles established by the Constitution. In essence, it enforces the respect and protection of the rights of children as guaranteed by the Constitution. The Family Code specifies the rights and obligations of family members, with a particular focus on the rights of children as essential subjects in family relationships. In accordance with the Constitution and the Family Code, children have the right to special protection and to enjoy their human rights and fundamental freedoms adapted to their age and maturity. The Family Code precisely regulates the rights of children in the family environment and their rights to protection against all forms of exploitation and abuse. Moreover, the Family Code extensively addresses the situation of children and minors for whom parents cannot provide care, children without parental care, and those who require special protection from the state. In connection with the challenges of the digital age, the Family Code also establishes important foundations and guidelines for protecting the rights of children in the digital environment. Based on these guidelines, safeguards are put in place to protect children from potential dangers posed by the digital age. This is crucial as children in modern society are increasingly turning to the use of digital devices and the Internet.

21 Akt o potrditvi nasledstva glede konvencij, statutov in drugih mednarodnih sporazumov, ki predstavljajo akt o ustanovitvi mednarodnih organizacij, Uradni list RS, št. 35/92.

22 Erjavec, 2014, p. 5.

23 Zakon o ratifikaciji Evropske konvencije o uresničevanju otrokovih pravic (MEKUOP), Uradni list RS, št. 86/1999.

24 Art. 57 of the Constitution of Republic of Slovenia.

25 Basic School Act, Uradni list RS, št. 81/06 – uradno prečiščeno besedilo, 102/07, 107/10, 87/11, 40/12 – ZUJF, 63/13, 46/16 – ZOFVI-K in 76/23.

The Slovenian legislator has anticipated several acts regulating relationships, as well as the rights and obligations of individuals in the digital environment. The new Personal Data Protection Act,²⁶ which replaced the existing one in January 2023 and regulates substantive areas within national jurisdiction as stipulated by the General Data Protection Regulation²⁷ (hereinafter: GDPR), together with the provisions of the GDPR, establishes rules for the collection, processing, and storage of personal data, which is particularly important when it comes to children's data. GDPR Article 6 para. 1 sets out the legal bases for the processing of individuals' personal data. One of the legal bases for processing personal data is the individual's consent, in accordance with Article 6 para. 1 point a) of the GDPR. When personal data is processed based on a child's consent regarding information society services, the GDPR sets the age limit at 16 for valid consent. However, Member States can independently set a lower age, provided it is not lower than 13 years. In Slovenia, consent for the use of information society services offered directly to children or services that are likely to be used by children is valid if the child is 15 years or older. If the child is under 15, consent is valid only if given or approved by one of the child's parents, their guardian, or the person granted parental care. When an information society service is offered free of charge, consent may also be granted by a foster parent or a representative of the institution in which the child is placed. In cases where the terms of service of the information society service provider prescribe a higher age for a child to use these services, the age from these terms of service is considered. The child's consent must not be conditioned by excessive requirements from the controller that require the child to provide more personal data than necessary for the purpose of such an activity.²⁸

When discussing the position of children in the digital age, it is essential to mention the Electronic Communications Act²⁹ and the Consumer Protection Act. The Electronic Communications Act regulates the use of electronic communications, including the Internet, establishes rules for online privacy protection, and provides certain protective mechanisms to prevent unauthorised access to children's communications online. In addition, the Consumer Protection Act addresses the position of consumers and specifies that providers of digital services must ensure a high level of consumer protection, including for children. This means that digital platforms designed for or used by children must be structured to provide a safe and appropriate online environment for them.

Moreover, if the relevant legislation does not provide adequate legal protection for the child, parents can invoke Article 134 of the Obligations Code³⁰ and file a request to cease violations of their children's personality rights. Everyone has the right to demand from a court or another competent authority to order the cessation of actions

26 Personal Data Protection Act, Uradni list RS, št. 163/22.

27 European Parliament and the Council, 2016.

28 Article 8 of the Personal Data Protection Act.

29 Electronic Communications Act, Uradni list RS, št. 130/22 in 18/23 – ZDU-10.

30 Obligations Code, Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631.

violating the inviolability of a person's personality, personal and family life, or any other personality right, to prevent such actions, or to remove their consequences. If the violator does not stop such behaviour, they must pay a specified amount to the affected party. Parents can refer to this provision even in cases where someone on the Internet unjustifiably publishes content related to a child.

2. Children's Rights on Internet Platforms

2.1. The Right to Privacy and the Right to Be Forgotten

The right to privacy is a fundamental human right, including the rights of children, regulated both at the international and constitutional levels, protecting the child from state authority, the public, and individuals. The right to privacy encompasses decisional, mental, spatial, and informational privacy.³¹ Slovenia, on the international level, has incorporated the Universal Declaration of Human Rights³² into its legal system, defining the right to protection against arbitrary interference with private life in Article 12. Additionally, the Convention on the Rights of the Child, through Article 16, ensures children the right to legal protection against arbitrary or unlawful interference with their private life, family, home, or correspondence, as well as against unlawful attacks on their honour and reputation. In Slovenia, the right to privacy is further safeguarded by the International Covenant on Civil and Political Rights,³³ adopted in 1992, which obliges member states to ensure civil and political rights. The European Convention on Human Rights³⁴ also protects human rights and fundamental freedoms.³⁵ At the national level, Article 35 of the Constitution protects the right to privacy and personal rights. It ensures the inviolability of human physical and mental integrity, privacy, and personal rights, including one's own image. When considering the right to privacy of children, Article 35 of the Constitution should be interpreted in conjunction with Article 56 of the Constitution, which stipulates that children enjoy human rights and fundamental freedoms in accordance with their age and maturity.

With the development of digitisation, social media, and websites, there is often a disclosure of personal data and other private information of individuals, which is particularly problematic when individuals, especially children, have insufficient awareness of how the Internet works and its pitfalls. However, parents are the ones who have a wealth of information about their children and may consequently (excessively) expose them, for example, by posting visual material, disclosing health conditions, information about behaviour, and the like. Respecting the right to privacy in the relationship between parents and children can be very problematic because the

31 Lampe, 2004, p. 42.

32 United Nations General Assembly, 1948.

33 United Nations General Assembly, 1966.

34 Council of Europe, 1950.

35 Stopar, 2018, pp. 32–33.

posts reveal the child's privacy without their consent. Currently, there are no explicit legal provisions in Slovenia restricting parents from posting children's personal data online, so there is a sense that children's right to privacy is often overlooked.³⁶ According to the law in Slovenia, children acquire limited legal capacity only when they reach the age of 15, while they gain full legal capacity upon reaching the age of 18 or earlier in cases specified by law. Consequently, children under the age of 15 cannot enforce legal remedies against violations of their privacy through online posts. Within the framework of parental care, parents are not restricted in sharing their children's data with the public. However, they must consider the legal limitation set by Article 7 of the Family Code, which stipulates that parents must, in all activities related to the child, ensure the child's best interests. In certain situations, parents may not be aware that they are violating the child's right to privacy. According to the Ombudsman of the Republic of Slovenia (hereinafter: Ombudsman), the publication of photos and personal data of children today does not constitute such a threat to children that would justify state intervention in the family.³⁷ Parents must nevertheless exercise maximum restraint when intervening in a child's privacy of this nature and allow the child to decide on an appropriate approach as they mature. The issue becomes further complicated in cases where parents do not agree. The Ombudsman believes that parents should decide unanimously on the public sharing of children's photos, and if such consensus is lacking, abstaining from posting is necessary.³⁸

Violations of a child's privacy can also occur through the actions of journalists and the media in general, particularly with the publication of photographs and other personal data of children. Increasingly, there are reports about children who are victims of violence or are involved in legal, administrative, or other proceedings because of family circumstances. Exposure in media reporting can harm the child. Therefore, the Criminal Code defines the publication of personal data of children involved in legal proceedings as a criminal offence.³⁹

The right to be forgotten is, by contrast, a more recent legal concept that is of paramount importance for the protection of personal rights and data in the digital age.⁴⁰ In Slovenia, the right to be forgotten is regulated by the GDPR, which, through Article 17, allows individuals to request the erasure of their personal data from data controllers without undue delay, assuming the conditions for erasure from the same article are met. The Slovenian Personal Data Protection Act refers to the GDPR regarding the right to be forgotten and stipulates that an individual can seek judicial protection throughout the duration of the violation, without prior exercise of rights under other provisions of the law or the use of other legal remedies.⁴¹ Slovenian legislation does not have specific provisions related to a child's right to be forgotten. Article 8 of

36 Ibid.

37 Ibid.

38 Varuh človekovih pravic, 2016.

39 Dolčič, 2014, p. 65.

40 Drobež, 2020, pp. 41–43.

41 Art. 11 of the Personal Data Protection Act.

the Data Protection Act specifies that the consent of a child for the use of information society services offered directly to children, or for which it can be presumed that children will use them, is valid if the child is 15 years or older.

The GDPR does not require the service provider to verify whether a user claiming to be underage and unable to give consent on their own (in accordance with the laws of a member state) is old enough. However, it clearly states that processing the data of children who are not old enough is illegal. The service provider is not obligated to verify a user's claims about their age, but they must verify whether a parent has given further consent or approval. When verifying age, it is important to avoid unnecessary data processing and to be proportionate to the risk posed by the proposed processing. In low-risk cases, a simple statement from the user may be sufficient. Once a child reaches the prescribed age, the consent given by the parent can be revoked in accordance with Article 7(3) of the GDPR, and they also have an "unconditional" right to erasure under Article 17 para. 1 point f).⁴² When it comes to collecting personal data as part of the offer of information society services in accordance with Article 8 para. 1, the controller must immediately delete this personal data in a manner that does not allow for delay. In this case, the right to erasure is entirely mandatory and independent of other conditions. Despite the right to be forgotten that a child can exercise when they become legally competent, it is necessary to consider the harm that such an action can cause to the child when posting information online.

2.2. The Right of Access to Information and the Right to Education

The right to access information is subject to convention protection in Slovenia. Slovenian legislation does not have specific provisions regarding children's rights concerning access to information. Article 17 of the Convention on the Rights of the Child emphasises the important role of the mass media and ensuring access to information and materials from various domestic and international sources, especially those aimed at enhancing the child's social, spiritual, and moral well-being, as well as physical and mental health. To this end, member states are encouraged to disseminate information beneficial to children, engage in international cooperation, create children's books, consider the needs of children from minority language groups, and develop guidelines for protecting children from harmful content. In Slovenia, the right to access information is predominantly exercised in connection with the right to education. The Ombudsman informs children and young people about their rights and provides support through online information, email, phone contact, in-person assistance, postal services to the institution's address, brochures, posters, bulletins, and similar means. The Slovenian police (among other institutions) provide a website specifically designed for children. This platform offers information on online safety and abuse. In addition, the Public Information Access Act⁴³ enables citizens to access

42 European Data Protection Board, 2018, pp. 25–27.

43 Public Information Access Act, Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US, 102/15, 7/18 in 141/22.

information held or controlled by public authorities, institutions, and other entities of public law. The law outlines the framework for information available to the public and the access procedure. The purpose of this regulation is to ensure transparency in the functioning of entities and to promote citizens' right to obtain information. Slovenia is also bound by the provisions of the GDPR, which, in Articles 13 and 14, imposes an obligation on data controllers to provide individuals whose personal data they process with information about the processing. Furthermore, the GDPR stipulates that data controllers must ensure that information presented to children is in a clear and understandable language adapted to their age. This implies that the information should be simple, clear, and tailored to the age of the children.

The conventional right to education is one of the fundamental rights of children, carrying broad societal and legal significance, and providing individuals with access to education crucial for their personal and social development. The Constitution guarantees freedom of education in Slovenia, where primary education is compulsory and funded by public resources, thus maintaining religious and political neutrality. It is the state's duty to create opportunities for citizens to acquire appropriate education.⁴⁴ In line with the Constitution, the education of children is the right and duty of parents, subject to limitation or withdrawal only for the benefit of the child.⁴⁵ Consistent with the constitutional principles of a democratic and social state, the state must create opportunities for citizens to obtain relevant education.⁴⁶ Therefore, every child has equal access to appropriate education, meaning they can participate under the same conditions in all forms of education. The state is obligated to provide material and other resources to establish and operate schools.⁴⁷ In summary, individual education rights in the Slovenian legal system are governed by over a hundred different legal acts. Education is not just an individual's right but also a responsibility of the state, where access to various forms of education is crucial for equality, the development of children, and societal progress.

2.3. The Right to Be Safeguarded From Abuse

The Convention on the Rights of the Child prohibits any form of child abuse. Slovenia, through Article 19 of this convention, is committed to safeguarding children from all forms of abuse, violence, harm, neglect, torture, or exploitation through appropriate legislative, administrative, social, and educational measures while the child is under the care of parents, legal guardians, or other individuals responsible for their well-being. In accordance with Article 56 of the Constitution, children are provided with special protection against economic, social, physical, mental, or other exploitation and abuse. The primary task of the family is the successful socialisation of children, and therefore, the criminalisation of domestic violence with the Domestic Violence

44 Art. 57 of the Constitution of the Republic of Slovenia.

45 Ibid., Art. 54.

46 Kocjančič, 2009, p. 132.

47 Kaučič, 2008, p. 152.

Prevention Act⁴⁸ sends a clear message of the state's rejection of such behaviour. When anomalies occur in family relationships, the state has the right and duty to intervene and protect its most vulnerable members who, due to their age and level of maturity, cannot care for themselves.⁴⁹ Moreover, the safety of children online has become one of Slovenia's key concerns, particularly in preventing abuse and ensuring a secure online environment for children. Based on international and national trends and guidelines, the Slovenian legislator has established specific provisions for the protection of children in the online environment.

Children must have the opportunity to receive education (including online or through other content) and access information. However, their access to information must be restricted when certain content could harm them. Such limitations to access certain content, for example, are determined by the Audiovisual Media Services Act,⁵⁰ which is the fundamental law that defines the rights, obligations, and responsibilities of legal and natural persons engaged in the provision of audiovisual media services (via television) and video-sharing platform services.⁵¹ Article 10 of the Audiovisual Media Services Act stipulates that special protection is provided to children and minors. The interests of children and minors take precedence over all other rights and judgements. Through audiovisual media services, it is prohibited to affect the physical, mental, or moral development of children and minors. No child or minor should be exposed through audiovisual media services to arbitrary or unlawful interference in their private life, family, or home, nor to unlawful attacks on their honour and reputation. Content that could harm the physical, mental, or moral development of children must be categorised appropriately, indicating for which age group the content is unsuitable. Providers of audiovisual media services must publish an appropriate acoustic and visual warning regarding content unsuitability for a specific age before broadcasting begins. During broadcast, the content must be constantly marked with an appropriate visual symbol. Content not suitable for children (adult content) must be protected by technical means (password) to ensure that children generally cannot hear or see it.⁵² Providers of audiovisual media services must establish rules of conduct designed to enable children to develop healthy eating habits.⁵³

Children are also specifically protected in the field of advertising content. In the field of consumer protection, the Consumer Protection Act, in Article 40, specifies that advertising must not contain elements that cause or could cause physical, mental, or other harm to children, or elements that exploit or could exploit their trust or lack of experience. Furthermore, Article 41 stipulates that all advertising messages that are part of or represent an information society service must be clearly recognisable

48 Domestic Violence Prevention Act, Uradni list RS, št. 16/08, 68/16, 54/17 – ZSV-H in 196/21 – ZDOsk.

49 Javornik Novak, 2014, p. 137.

50 Audiovisual Media Services Act, Uradni list RS, št. 87/11, 84/15, NPB1, 204/21 in NPB2.

51 Ibid., Art. 1 of the Audiovisual Media Services Act.

52 Ibid., Art. 14.

53 Ibid., Art. 23.

as advertising messages. If advertising in an advertising message directly addresses children to purchase the advertised product or persuades parents or other adults to buy the advertised product for children, such advertising would be considered an unfair aggressive business practice. If a company uses unfair business practices and thereby causes harm to a consumer, the consumer can demand a price reduction or terminate the contract and request a refund of the amount paid. The consumer can also seek compensation for damages from the company under general rules of liability for harm.⁵⁴ Unfair business practices are assessed by the court, as well as the Market Inspectorate of Slovenia and other competent inspection authorities.⁵⁵

The Mass Media Act⁵⁶ also contains provisions aimed at protecting children's moral, physical, and mental integrity. Article 49 of the Mass Media Act stipulates that media houses must ensure the protection of minors from content that could harm their health or development. This includes restrictions on displaying violence, pornography, inappropriate language, and other content that could be harmful to children. Access to pornographic content in electronic publications must also be technically restricted to prevent children from accessing it.⁵⁷

An important part of child protection is, therefore, restricting their access to content that could harm them. If children, despite these restrictions, become victims of online harassment, such as insults, threats, or the posting of photos or videos (real or altered), they have the right (through their parents or other institutions) to demand that such harassment ceases. Often, the police are also the appropriate authority in such cases.

2.4. The Right to Freedom of Expression and the Right to Be Heard

The Convention on the Rights of the Child recognises the right of children to freedom of expression, encompassing the freedom to seek, receive, and impart all kinds of information and ideas, regardless of frontiers, in oral, written, printed, or artistic form, or by any other means chosen by the child. This right is limited only by the respect for the rights and reputation of others and the protection of state or public security. The state must respect the child's right to freedom of thought, conscience, and religion, along with the related rights of parents or legal guardians.⁵⁸ The right to freedom of expression is defined in various laws and subordinate regulations in the Slovenian legal system across different areas. Particularly noteworthy is Article 39 of the Constitution, which guarantees everyone the freedom of expression of thought,

54 Art. 55 of the Consumer Protection Act.

55 Ibid., Art. 57.

56 Mass Media Act, Uradni list RS, št. 110/06 – uradno prečiščeno besedilo, 36/08 – ZPOmK-1, 77/10 – ZSFCJA, 90/10 – odl. US, 87/11 – ZAvMS, 47/12, 47/15 – ZZSDT, 22/16, 39/16, 45/19 – odl. US, 67/19 – odl. US in 82/21.

57 Art. 84 of the Mass Media Act. In accordance with Art. 176 of the Criminal Code, anyone who displays, or in any other way provides access to, objects of pornographic content to a person under the age of fifteen shall be punished.

58 Arts. 13–14 of the Convention on the Rights of the Child.

speech, public appearance, printing, and other forms of public informing and expression. Everyone is free to gather, receive, and disseminate news and opinions. The Ombudsman emphasises the need for the state to ensure that the child's perspectives are effectively heard in legal proceedings, stressing the necessity to expand the system of a child's advocate. This commitment is enshrined in laws that regulate individual procedures, including the Placement of Children with Special Needs Act.⁵⁹ A child should never be merely an object of a specific legal procedure determining their rights and duties based on the opinions of parents, teachers, and other experts. Despite the fact that children may not comprehend all decisions due to their psychophysical characteristics, it should not be taken for granted that their parents or guardians will always decide in their best interest, even though it is their duty and right according to the Family Code.⁶⁰ Due to observations of insufficiently equipping children with relevant information, not involving children in problem-solving, and disregarding the distinctiveness of their perception, Slovenia has established a system of child advocacy. This allows children involved in proceedings determining their rights and interests to have an advocate appointed. The Ombudsman is the one who assesses whether the conditions for appointing an advocate exist.⁶¹ Slovenia strives to ensure that children's perspectives are genuinely heard and considered, enhancing the child's position in proceedings and striking a balance between expressing opinions and safeguarding the child's interests in various legal situations.

In Slovenia, the right of the child, which is directly connected to the right of children to freedom of expression, is also realised – the right to be heard. In the Slovenian context, there is an increasingly established awareness that the right to be heard as a child is primarily a right and not a duty. With the legal institution of the child advocate, Slovenia has implemented Article 12 of the Convention on the Rights of the Child into practice. This article stipulates that states ensure the right of the child capable of forming their own views to freely express those views.⁶² The Ombudsman strives for children to be heard in proceedings and matters that determine their best interests. The child advocacy institution is based on the child's consent and strengthens the voice of the child. It relies on trust between the child and the advocate, ensuring that the child's opinion is conveyed to those who need to hear it – such as courts, social work centres, and other authorities deciding on the child's future. This right applies to all proceedings related to the child. The advocate not only conveys the child's opinion but helps the child recognise their own wishes and needs, enabling a safe expression of experiences, emotions, and perceptions. It is essential to distinguish that the advocate is not the legal representative of the child, a court expert, or an extended arm of other institutions, but operates independently in their role.⁶³ So far, the child advocate

59 Placement of Children with Special Needs Act, Uradni list RS, št. 58/11, 40/12 – ZUJF, 90/12, 41/17 – ZOPOPP in 200/20 – ZOOMTVI.

60 Dolčič, 2014, pp. 59–62.

61 Jenkole, 2006, p. 35.

62 Javornik, 2021, pp. 13–13.

63 Ruparčič, 2021, pp. 6–10.

has most often been appointed in proceedings related to divorce, the reallocation of the child, changes in visitation, removal of the child from the family and placement in institutional or foster care, and regarding visits in foster care.⁶⁴ The right of children to be heard is also important from the perspective of exercising civil rights. In Slovenia, children do not have the right to vote, as it is reserved for citizens who have reached the age of 18. Therefore, it is even more important for adults to listen to and consider the voices of children. Considering this, Slovenian organisations and institutions are joining various projects to increase opportunities for children's participation. Recently, Slovenia participated in the Council of Europe's CP4Europe project, aimed at strengthening and promoting children's rights to participate at the national and pan-European levels.⁶⁵ Participation of children is also encouraged in the school environment in Slovenia. Educational institutions provide space for expressing opinions and ideas and involve children in decisions that affect their school environment. In the Slovenian context, there is an awareness that the right of children to be heard is crucial for their holistic development and the realisation of their rights.

3. Presentation of the Case Law in the Area Concerned

3.1. Case 1: Admissibility of Online Content

Ljubljana Higher Court assessed⁶⁶ the admissibility of online content publication related to children by one of the parents (with the objection of the other parent). During the proceedings, the court prohibited the defendant (mother or custodian) from publishing and disseminating already published content related to their under-age children on all social media platforms. The court also ordered her to immediately delete the already published content on social media. The defendant appealed against the decision.

The court clarified that when parents do not reside together, and the child is not entrusted to the care and upbringing of both parents (as in the present case), decisions regarding the daily life issues of the children are made by the parent to whom the children are entrusted for care and upbringing. On matters significantly affecting the development of the children, the parents make decisions through mutual agreement and in accordance with the best interests of the children. If parents, even with the assistance of the social welfare centre, cannot reach an agreement on issues significantly affecting the development of the children, the court makes the decision.⁶⁷ A temporary order regarding the issue of posting content about children on social media is a provisional decision of the court on a matter significantly affecting the development of the children, on which the parents (apparently, even with the assistance of

⁶⁴ Varuh človekovih pravic, 2019.

⁶⁵ Council of Europe, n.d.

⁶⁶ Ljubljana Higher Court, Sklep IV Cp 1440/2020, 21 September 2020.

⁶⁷ Art. 151 of the Family Code.

the social welfare centre) could not reach an agreement, as the appellant was posting and disseminating content about the children, while the plaintiff objected to it.

The court agreed with the plaintiff's assertion that the children are recognisable in the environment where they live. This is true to a certain extent for all individuals, but unfortunately, it is even more so for the children of the parties involved in the dispute. The court explained that the more concerning aspect of recognition is caused by the writing and posting of other content about the children on social media. This exposure, as commonly known, is much broader and potentially more far-reaching, and due to the nature of social networks, it can even be permanent. Therefore, it has a stronger and more lasting impact on the lives of children. The appellate court concurred with the first-instance court's finding that the right of children to respect for their private and family life and the concern for their healthy growth and harmonious personal development take precedence over the parents' right to express themselves (about their children) on social media. The appellate court did not find any short- or long-term benefits that children could derive from the publication of content about them on social media, not only in the specific situation or for the specific children but in general. The court stated that widely informing the community through social media exposes children, who are already vulnerable due to their age and their parents' separation, to the public in the long term, and this alone poses a (long-term) threat to them. Simultaneously, they may face comments and reactions from people they encounter, which could cause them severe distress, endangering them both in the short term and the long term. The Child Welfare Centre also assessed that media exposure endangers children. The appellate court found that the posts by the mother/custodian endangered the children, so the decision of the first-instance court to issue a temporary injunction was appropriate.

3.2. Case 2: Posting Photographs and Videos of the Underage Child

In the case VSL Decision IV Cp 105/2021,⁶⁸ the justification of the issued interim injunction was under consideration. The injunction prohibited the plaintiff (mother or custodian) from posting photographs and videos of the underage child on all social media platforms, especially on Facebook, TikTok, Instagram, and YouTube. The court ordered her to immediately remove all previously posted photographs and videos on the mentioned platforms. In the event of a violation of the issued interim injunction, a monetary penalty in the amount of EUR 300 was stipulated.

The plaintiff filed an appeal, contending that the issue of posting photos and videos of the child on social media is not a matter significantly affecting the child's development, and therefore, it is not a matter on which the parents should reach mutual agreement. She argued that the child had been entrusted to her care and upbringing. She stated that the matter is of a daily nature, and as such, she has the full right to independently decide on the publication of photos depicting the child's everyday life. In the twenty-first century, she noted, social media and postings have become

68 Ljubljana Higher Court, VSL Sklep IV Cp 105/2021, dated 22 February 2021.

entirely commonplace, and her posts of the child do not pose any threat whatsoever. She further asserted that the plaintiff's claims are merely general statements alleging potential risks of the global internet and possible misuse. The plaintiff emphasised that especially during the then-prevailing epidemiological conditions and the need for remote schooling, virtually all children were inevitably exposed to the online world, where sensitive personal data and photographs are also transmitted.

The Higher Court concurred with the plaintiff's assertion that the condition of a likely demonstrated endangerment of the child is not fulfilled. According to the opinion of the Higher Court, the defendant did not likely demonstrate that the plaintiff's posts (photographs and videos) would jeopardise the child's interests and, therefore, necessitate protection through an interim injunction. The court issues an interim injunction when it is demonstrated that the child is likely endangered.⁶⁹ In accordance with the second paragraph of Article 157 of the Family Code, a child is considered endangered if they have suffered or are highly likely to suffer harm, and this harm or the likelihood of its occurrence is a result of the acts or omissions of the parents or a consequence of the child's psychosocial problems manifested as behavioural, emotional, learning, or other issues in their upbringing. The mentioned harm includes damage to the physical or mental health and development of the child or to the child's property.⁷⁰ The court clarified that any posting of photos and videos on social media does not automatically constitute a threat to the child's interests. Merely the (potential) possibility that such posts of photos and videos on social media could pose a threat (in the future) does not meet the condition of a demonstrated likely endangerment of the child.

3.3. Case 3: Postings on Social Media of the Child

In the case VSL Decision IV Cp 2105/2021,⁷¹ the Higher Court also assessed whether postings on social media endanger the child. The mother, on her profile, the company profile, and profiles of third parties on the Instagram and Facebook social media platforms, posted photographs of her three-year-old daughter. In certain photos, the child was only in swimwear, revealing her complete appearance, including her face, making her easily identifiable. The father did not consent. The content was published in a manner accessible to everyone, written in English, and included hashtags, facilitating rapid dissemination on the internet. The content was also posted with the intention of promoting a brand. Consequently, the first-instance court concluded that the dissemination of such personal and confidential content online, where the publication can reach virtually anyone, poses a threat to the child. Exposure to such content may cause her mental distress and make her vulnerable to abuse.

The Higher Court concurred with the first-instance court's conclusion that the publication of photos and videos allowing the identification of a child infringes upon

69 Art. 161 of the Family Code.

70 Ibid., Art. 157 para. 3.

71 Ljubljana Higher Court, VSL Sklep IV Cp 2105/2021 dated 5 January 2022.

their right to their own image as an integral part of the right to privacy. It also agreed with the assessment that posting photos and videos of children on social media increases the risk of potential abuse of the child. However, this alone is not sufficient to establish a likely demonstrated causal link between any photo publication of the child and harm to their health and development, let alone the occurrence of irreparable harm necessitating immediate intervention. The opinion of the Ombudsman also indicates that the decision of parents to post photos of their children online falls under decisions that can significantly influence a child's healthy development, and therefore, their consent is generally required. However, it does not constitute such a threatening action to the child that would invariably warrant state intervention in the family relationship.

3.4. Case 4: Disclosure of Personal Data

The Higher Court, in the judgement II Cp 693/2018,⁷² addressed the contentious post by the defendant, who published on the Facebook platform a disclosure revealing the name, surname, and address of the plaintiff, and the fact that she was taking care of two vulnerable boys. The post pertained to a highly publicised removal of the two boys, for whom the parents were no longer able to care, and they were staying with the grandmother at the time of removal. After the removal, the boys were placed in a foster family (that of the plaintiff). The court clarified that the fundamental function of foster care is to nurture and raise the child, performing certain duties that parents would otherwise have within the scope of parental rights. The primary principle of guardianship is to pursue the best interests of the child. Therefore, a foster family is also considered a family, and the privacy of its members (including the foster mother) is protected to the same extent as the privacy of other families. However, the uniqueness of foster families lies in their acceptance of children whose interests are endangered, requiring special care. Consequently, the privacy of their family life is even more sensitive. The publication of the names, surnames, address, and the fact that the boys in question were with the plaintiff constitutes a serious intrusion into the plaintiff's privacy.

3.5. Case 5: Offensive and Vulgar Content

In the decision VSL Decision I Cp 1189/2021,⁷³ the Higher Court clearly expressed its position regarding the posts of both parties, stating that both former partners, being aware that their online posts contain offensive and vulgar content accessible to anyone (including their children), should, in the future, carefully consider the consequences that their publicly hostile confrontations may have on their children.

72 Ljubljana Higher Court, VSL Sodba II Cp 693/2018 dated 3 October 2018.

73 Ljubljana Higher Court, VSL Sklep I Cp 1189/2021 dated 1 September 2021.

3.6. Case 6: Protected Privacy of a Minor

The Supreme Court of the Republic of Slovenia, in the judgement VSRS Decision I Ips 12291/2012,⁷⁴ clarified that in criminal proceedings where, according to the law, public access is excluded, the privacy of a minor is protected to the extent that information about the proceedings cannot be published without the court's permission, even if the minor or their parents consent to the publication of such information. The purpose of the provision in the second paragraph of Article 287 of the Criminal Code is to protect and safeguard the privacy of children, especially when a child is exposed to media coverage, even at the request or with the consent of the parents. The purpose of legal provisions is to prevent deliberate and gross violations of children's rights to privacy and their personal rights, particularly in sensationalist media reporting. The guiding principle in legislation is to ensure the protection of the best interests of the child in all proceedings and activities related to children.

3.7. Summary of Cases

To sum up, the first three cases revolve around a substantially similar issue of publishing photographs and videos of children on websites or social media platforms. In these initial three cases, a common concern is evident among one of the parents that the publications could harm or jeopardise the child's welfare. Typically, it is clear that both parents should consent to the publication of photos of a child online because it is a decision that significantly influences a child's healthy development. However, the mere act of publishing a child's images does not necessarily imply that the child is endangered, nor does it automatically warrant state intervention in family relationships. The determination of whether a child is genuinely at risk due to the publication is assessed on a case-by-case basis. Nevertheless, from the analysis of these legal proceedings, it can be inferred that parents are increasingly aware of the importance of protecting children's rights in the online environment.

In the fourth case, the significance of safeguarding privacy, especially in foster family relationships, is explained. The fifth case serves as a reminder to parents about the harm their statements can cause to children, highlighting the court's meticulous attention to the protection of children's interests. Lastly, the sixth case illustrates the protection of children's privacy in criminal proceedings, taking into consideration the potential harm that media publications could inflict on minors.

4. Protecting Children in the Digital Space: The Role of Public Institutions, Legal Remedies, and Education in Public Schools

Several public institutions and authorities in the Republic of Slovenia are responsible for protecting children's rights online.

⁷⁴ Supreme Court of the Republic of Slovenia, VSRS Sodba I Ips 12291/2012 dated 1 February 2018.

The Ombudsman represents a constitutional category that does not fall within the executive, judicial, or legislative branches of government. The Ombudsman does not operate as part of the government mechanism but acts as its overseer, limiting its arbitrariness in encroaching on human rights and fundamental freedoms. The Ombudsman operates independently and autonomously in relation to other state bodies. The Ombudsman's jurisdiction is not limited to direct violations of the human rights and freedoms set out in the Constitution; the office is also responsible for addressing any violations of individuals' rights by public authorities.⁷⁵

The Ombudsman ensures the protection of individuals, including children, by investigating their complaints and, if the complaints are justified, recommending corrective actions. Anyone who believes that their human rights or fundamental freedoms have been violated by an act or action of a state authority, local community authority, or public authority can file a complaint with the Ombudsman to initiate an investigation.⁷⁶ State authorities, local community authorities, and public authorities must provide the Ombudsman with all data and information within their jurisdiction upon request, regardless of the level of confidentiality, and allow for investigations; otherwise, fines can be imposed.⁷⁷ In the final report, the Ombudsman provides their assessment of the facts and circumstances of each individual case, determining whether there has been a violation of human rights or fundamental freedoms and how they were violated, or if there was any other irregularity. The Ombudsman does not interfere with the civil law rights that individuals have for compensation. Additionally, the Ombudsman can recommend the initiation of disciplinary proceedings against employees of authorities who have caused the identified irregularity.⁷⁸ Authorities must inform the Ombudsman about the actions taken based on their suggestions, opinions, criticisms, or recommendations; otherwise, the Ombudsman can report this directly to the superior authority, the relevant ministry, report it to the National Assembly in a special report, or publicly disclose the matter.⁷⁹

The Agency for Communication Networks and Services of the Republic of Slovenia (AKOS) is an independent authority that regulates and supervises the electronic communications market, manages and monitors the radiofrequency spectrum in Slovenia, performs tasks in the field of radio and television activities, and regulates and supervises the market of postal services and railway transport services in Slovenia.⁸⁰ AKOS is also responsible for monitoring violations of the provisions of the Audiovisual Media Services Act and can impose fines on violators.

75 Varuh človekovih pravic, n.d.

76 Art. 26 of Human Rights Ombudsman Act, Uradni list RS, št. 69/17 – uradno prečiščeno besedilo.

77 Ibid., Arts. 6 and 56.

78 Ibid., Art. 39.

79 Art. 40 of the Human Rights Ombudsman Act.

80 Agencija za komunikacijska omrežja in storitve Republike Slovenije (n.d.) O agenciji [Online]. Available at: <https://www.akos-rs.si/o-agenciji> (Accessed: 30 November 2023).

The Information Commissioner of Slovenia is a supervisory authority responsible primarily for violations of the Personal Data Protection Act, the Public Information Access Act, and the GDPR. The Information Commissioner can initiate an inspection procedure, require the rectification of irregularities, and impose fines on the violator. The Information Commissioner is not competent when the violation is committed by a natural person within the scope of their purely personal or domestic activities.

Regarding the protection of children in the digital environment, it is essential to highlight the involvement of the police, the judiciary, and the Centre for Social Work. In the field of child protection in the digital environment, the police investigate criminal offences such as stalking, threats, unauthorised wiretapping and audio recording, unauthorised video recording, abuse of personal data, display, creation, possession, and dissemination of pornographic material, extortion, cyberattacks, and public incitement to hatred, violence, or intolerance.⁸¹ It is important to note that all state authorities and organisations with public authority must report criminal offences that are subject to prosecution *ex officio* if they become aware of them or otherwise learn of them.⁸² Furthermore, in accordance with Article 15.a of the Criminal Code, in cases where a criminal offence against life and body, against human rights and freedoms, against sexual integrity, or any other offence under this Code with signs of violence is committed against a minor, the perpetrator is prosecuted *ex officio*. This further reinforces the obligation of all state authorities and organisations with public authority to report criminal offences. The police also engage in advisory and awareness-raising activities.

Children's rights are also safeguarded by social welfare institutions, including the Centres for Social Work. Authorities, institutions, and other organisations that identify the endangerment of a child, a minor, or a person deprived of legal capacity in their work are obliged to inform the Centre for Social Work in their area about it.⁸³ The court and the relevant Centre for Social Work intervene when it is necessary to protect the rights and interests of children. Measures to protect the interests of the child include temporary orders, emergency removal of the child, and more lasting measures. The court imposes measures to protect the child's interests if it determines that the child is at risk. The Centre for Social Work can propose measures to the court, participate in legal proceedings, and provide its opinion.

In raising awareness among children, adolescents, parents, and teachers about safe internet use and children's rights in the digital environment, various organisations play a significant role, such as the project Centre for Safer Internet.⁸⁴ The Centre for Safer Internet is a project implemented by the Faculty of Social Sciences at the

81 Arts. 134.a, 135, 137, 138, 143, 176, 213, 221 and 297 of the Criminal Code.

82 Art. 145 of the Criminal Procedure Act.

83 Art. 91 of the Social Assistance Act, 1992, Uradni list RS, št. 3/07 – uradno prečiščeno besedilo, 23/07 – popr., 41/07 – popr., 61/10 – ZSVarPre, 62/10 – ZUPJS, 57/12, 39/16, 52/16 – ZPPreb-1, 15/17 – DZ, 29/17, 54/17, 21/18 – ZNOrg, 31/18 – ZOA-A, 28/19, 189/20 – ZFRO, 196/21 – ZDOsk, 82/23 in 84/23 – ZDOsk-1.

84 See: <https://safe.si/center-za-varnejši-internet/o-centru> (Accessed: 30 November 2023).

University of Ljubljana, the Academic and Research Network of Slovenia, the Slovenian Association of Friends of Youth (ZPMS), and the Centre MISSS (Youth Information and Counselling Centre of Slovenia). The Centre for Safer Internet provides three main services:

1. The Awareness Centre Safe.si⁸⁵ operates with the aim of raising awareness among various target groups, including children, teenagers, parents, teachers, and social workers. This is achieved through various activities, such as online and offline events and lectures. The main purpose is to raise awareness about safe and responsible internet and mobile device use. Safe.si regularly collaborates with both primary and secondary schools. Some key content areas covered by the lectures include understanding fundamental concepts such as privacy, security, and responsibility online; recognising online dangers, cyberbullying, and harassment; the importance of thoughtful and responsible content sharing online; the use of secure passwords and their management; preventing the spread of false information; promoting respectful online communication and behaviour; and establishing family rules for internet and device use.
2. The National Network TOM⁸⁶ (Telephone for Children and Adolescents) is a publicly verified social welfare programme designed to prevent and address the social difficulties of individuals in vulnerable population groups. TOM is part of the ZPMS and was established in 1990 at the initiative of the Commission for Children's Rights at ZPMS. Through a toll-free telephone number (or online), young people can share their problems and obtain advice and additional information from counsellors, with guaranteed anonymity and confidentiality of the conversation. TOM also advises and assists young people with issues related to the Internet.
3. Spletno oko⁸⁷ is a Slovenian online reporting point where internet users can anonymously report child sexual abuse material or hate speech on the Internet. Over the course of 11 years of operation, it has received more than 22,000 reports believed to contain illegal hate speech or child abuse material. In over 2,000 cases, they identified the presence of actual illegal elements, which were then forwarded to the police for further action. Spletno oko, in collaboration with the police, the international organisation INHOPE, internet service providers, online portals, and other relevant government and non-governmental organisations, strives to reduce the presence of child sexual abuse materials and hate speech on the Internet.

85 See: <https://safe.si/> (Accessed: 30 November 2023).

86 See: TOM, telefon za otroke in mladostnike [Online]. Available at: <https://e-tom.si/> (Accessed: 30 November 2023).

87 Spletno oko, n.d.

The Slovenian Computer Emergency Response Team (SI-CERT) serves as the coordinator for resolving cybersecurity incidents and provides technical advice in cases of intrusions, computer infections, and other abuses. Additionally, it issues warnings to network administrators and the public regarding current threats on electronic networks. SI-CERT conducts the national awareness programme “Varni na internetu”⁸⁸ and collaborates on the SAFE-SI project. It operates under the auspices of The Academic and Research Network of Slovenia.⁸⁹

During primary education, children become acquainted with computer technology through an elective subject called Computer Science. In this subject, they learn about fundamental concepts of hardware and software, computer programs, word processors, data storage, email communication, web browsers, and more.⁹⁰ The primary school curriculum⁹¹ does not include a mandatory subject specifically dedicated to safe internet use or online dangers. These topics are introduced to children through the school’s efforts to incorporate them into their activities, which can also be achieved through collaboration with external organisations that conduct workshops and activities.

In February 2023, Slovenian primary school students achieved a Guinness World Record for the largest online quiz in the world. The quiz involved 20,000 Slovenian primary school students (with 15,225 participants answering all the questions) from nearly 200 schools. The quiz questions covered topics related to personal data protection, social networks, online violence, online empathy, and other challenges that young people encounter on the Internet. The quiz was organised by A1 and the Safe Internet Institute, as an extension of the programme “Spletne brihte”, through which the organisers have been educating children for two years about safe and responsible internet and digital technology use.⁹² It is evident that such topics are not unfamiliar to children, but schools need to be willing to incorporate these themes and activities into their educational process, as such lectures or content are not part of the mandatory curriculum.

Child protection on the Internet is generally not specifically legislated in Slovenia. As mentioned, the field is scattered across various laws. Certain content, such as television programmes, advertising, media contributions, and the like, is legally regulated with restricted access for children. However, on the Internet, general rules apply both for child protection and child protection online. The primary responsibility for child protection lies with parents, whose duty is to ensure the child’s well-being in all activities related to the child and to raise them with respect for their person, individuality, and dignity.⁹³ When it is determined that parents are not acting in the child’s best interest, the state may intervene. It is important to note that state

88 See: <https://www.varninainternetu.si/> (Accessed: 30 November 2023).

89 See: <https://www.cert.si/> (Accessed: 30 November 2023).

90 Batagelj, 2002.

91 Strokovni svet Republike Slovenije za izobraževanje, n.d.

92 Dnevnik, 2023.

93 Art. 7 para. 1 of the Family Code.

authorities, public service providers, holders of public authority, local government bodies, and other natural and legal persons must ensure the child's best interests in all activities and procedures related to the child.⁹⁴ Children enjoy special protection from the state whenever their healthy development is at risk and when other interests of the child demand it.

5. Summary

Slovenia has established a legal framework for child protection, but it is fragmented and somewhat lenient, especially regarding the Internet. The right to privacy is the most regulated, governed by the GDPR and the Personal Data Protection Act, which clearly state that organisations need a legal basis to process personal data. Unauthorised invasion of privacy can lead to court injunctions or compensation claims, and in some cases, criminal prosecution. Online and on social media, the legal basis for data processing is usually a contract, consent, or legitimate interest. Children are further protected here, as they cannot enter into contracts until a certain age. In line with general terms, children can typically create social media accounts when they turn 13. In Slovenia, a legal transaction (contract) made by a child under 15 is invalid. Considering the law, parental consent is required until the child turns 15 for creating an online account. In practice, this age restriction is often circumvented by stating a false birth year, either by the child or a parent. Article 8 of the GDPR is rarely applied in practice for social media use. For children, the legitimate interest of the controller is more stringently assessed under Article 6(f) of the GDPR. Court cases have shown disagreements among parents about online content shared by one parent, raising concerns about its impact on the child. There are worries that posting photos, videos, and other content featuring the child could harm or endanger them in the future. Courts have ruled that decisions to post on social media significantly influence a child's healthy development, but posting child images does not necessarily mean the child is endangered or that state intervention in family matters is needed. Whether a post actually endangers a child is judged case by case. Legally, child posts on social media are rarely unlawful unless they genuinely endanger the child based on actual circumstances. However, it is debatable whether parental posts of child content are beneficial, or if the decision should be left to the child upon reaching an appropriate age. The child's right to information or education is not precisely defined in Slovenian national legislation, but efforts by public institutions to provide clear and comprehensible information are evident. Ensuring a safe environment for children, both physically and virtually, is vital. Slovenian internet child protection involves numerous laws, mainly focusing on restricting access to certain content. While rules for limiting access to inappropriate content on TV or on-demand services are clear, children can generally access anything online. Restrictions apply to pornographic content and

94 Ibid., Art. 7 para. 4.

alcohol advertising, but verifying age online is rare, thus allowing easy access to inappropriate content. Children can also quickly become victims of cyberbullying, subject to the same legal standards as physical-world harassment. Parents primarily have the responsibility to act in the child's best interest and protect them appropriately. Other public institutions are obligated to intervene when parents fail. Children should have a safe space for expression, and their rights should only be limited when in their best interest. Slovenian legislation on internet child protection is lax, but court practices, guided by the child's best interest, fill the gaps. Education on safe internet use for both children and parents is crucial, as parents often underestimate the dangers of internet and social media use. There are no concrete legislative proposals in Slovenia for further protecting children's rights online. Everyone can contribute to a safe and friendly digital world by sharing positive content and reporting negative ones.

Bibliography

- Batagelj, V., et al. (2002) *Učni načrt, izbirni predmet, program osnovnošolskega izobraževanja, računalništvo, urejanje besedil, računalniška omrežja, multimedija*. Ljubljana: Ministrstvo za [olstvo, znanost in port, Zavod RS za olstvo [Online]. Available at: https://www.gov.si/assets/ministrstva/MIZS/Dokumenti/Osnovna-sola/Ucni-nacrti/izbirni/3-letni-lahko-krajsi/Racunalnistvo_izbirni.pdf (Accessed: 30 November 2023).
- Council of Europe (n.d.) 'CP4 Europe - Strengthening National Child Participation Frameworks and Action in Europe (EU-CoE Joint Project)', *Council of Europe Portal* [Online]. Project), at: <https://www.coe.int/en/web/children/cp4europe> (Accessed: 18 November 2023).
- Council of Europe (1950) European Convention for the Protection of Human Rights and Fundamental Freedoms, *Council of Europe Treaty Series*, No. 005.
- Dolčič, T. (2014a) 'Varuh človekovih pravic Republike Slovenije kot osrednja institucija za varstvo otrokovih pravic' in Jager Agius, I. (ed.) *Otrokove pravice v Sloveniji*. Ljubljana: Ministrstvo za zunanje zadeve, pp. 61–70.
- Dolčič, T. (2014b) 'Pravica otrok do svobodnega izražanja svojega mnenja', *Šolsko svetovalno delo*, 18(3-4), pp. 59–62.
- Drobež, E. (2020) 'Pravica do pozabe: tehtanje med svobodnim osebnostnim razvojem in svobodo poročanja', *Pravna praksa*, 39(26-27), pp. 41–43.
- Erjavec, K. (2014) 'P'redgovor' in Jager Agius, I. (ed.) *Otrokove pravice v Sloveniji, od normativnih standardov do učinkovitega varstva – Zbornik ob 25-letnici Konvencije o otrokovih pravicah, Zbirka Mednarodno pravo*. Ljubljana: Ministrstvo za zunanje zadeve, pp. 5–6.
- European Data Protection Board (2020) 'Guidelines on consent under Regulation 2016/679' [Online]. Available at: https://www.ip-rs.si/fileadmin/user_upload/Pdf/mnenja/Mednarodna_mnenja/mnenja_na_eu_ravni/20180416_WP259rev01_Article29WPGuidelinesonConsent.pdf (Accessed: 30 November 2023).
- 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).
- Javornik Novak, L. (2014) 'Zloraba otroka, Vloga zakonodaje, preprečevalnih ukrepov in družbene odgovornosti' in Jager Agius, I. (ed.) *Otrokove pravice v Sloveniji*. Ljubljana: Ministrstvo za zunanje zadeve, pp. 137–147.
- Javornik, L. (2021) 'Institut zagovornika kot oblika neposrednega uresničevanja konvencije ZN o otrokovih pravicah' in Steničnik, P. (ed.) *Izzivi in perspektiva zagovorništva otrok v Sloveniji*. Ljubljana: Varuh človekovih pravic, pp. 12–18.
- Jenkole, M. (2006) 'Zagovorništvo otrok in mladostnikov – to je naša obveza, in ne dobra volja!' in Jenkole, M. (ed.) *Zagovornik – glas otroka*. Ljubljana: Varuh človekovih pravic, pp. 35–39.

- Kaučič, I. (2008) 'Človekove pravice in svoboščine' in Kozarov, A. (ed.) *Ustavno pravo Slovenije*. Ljubljana: GV Založba, pp. 97–178.
- Kocjančič, R. (2009) 'Človekove pravice in temeljne svoboščine' in Kocjančič, R. (ed.) *Ustavno pravo Slovenije*. Ljubljana: Fakulteta za upravo, pp. 97–145.
- Kraljič, S. (2019) *Družinski zakonik s komentarjem*. Maribor: Poslovna založba Maribor.
- Lampe, R. (2004) *Sistem pravice do zasebnosti*. Ljubljana: Bonex založba.
- Oblak Črnič, T., et al. (2023) *Medijska kultura in digitalni vsakdan mladih: 1. del: Prisotnost, rabe in regulacija digitalnih tehnologij v družinah in šolah – Poročilo raziskave v okviru ARRS projekta Medijski repertoarji mladih (J5-2564)*. Ljubljana: Fakulteta za družbene vede. [Online]. Available at: https://medijimladih.si/wp-content/uploads/2023/03/MRM_porocilo_web.pdf (Accessed: 30 November 2023).
- Ruparčič, J. (2021) 'Zagovorništvo otrok kot posebna pozornost varuha' in Steničnik, P. (ed.) *Izzivi in perspektiva zagovorništva otrok v Sloveniji*. Ljubljana: Varuh človekovih pravic, pp. 6–11.
- Spletno oko (n.d.) 'Točka za prijavo posnetkov spolnih zlorab otrok na internetu' [Online]. Available at: <https://www.spletno-oko.si/> (Accessed: 30 November 2023).
- STA (2023) 'Slovenski osnovnošolci dosegli Guinnessov rekord za največji spletni kviz na svetu, *Dnevnik*, 16 February [Online]. Available at: <https://www.dnevnik.si/online/slovenski-osnovnosolci-dosegli-guinnessov-rekord-za-najvecji-spletni-kviz-na-svetu-2057554/> (Accessed: 30 November 2023).
- Stopar, U. (2018) 'Kršitev otrokove zasebnosti na spletu', *Pravna praksa*, 37(16-17), pp. 32–33.
- Strokovni svet Republike Slovenije za izobraževanje (n.d.) 'Programi in učni načrti v osnovni šoli' [Online]. Available at: <https://www.gov.si teme/programi-in-ucni-nacrti-v-osnovni-soli/> (Accessed: 30 November 2023).
- United Nations General Assembly (1948) Universal Declaration of Human Rights, 217 A (III), 10 December 1948.
- United Nations General Assembly (1966) International Covenant on Civil and Political Rights, adopted 19 December 1966, entered into force 23 March 1976, 999 UNTS 171.
- United Nations General Assembly (1989) Convention on the Rights of the Child, New York, 20 November
- Varuh človekovih pravic (n.d.) 'Podrobno o varuhu', *Varuh človekovih pravic* [Online]. Available at: <https://www.varuh-rs.si/o-varuhu/> (Accessed: 30 November 2023).
- Varuh človekovih pravic (2016) 'Zasebnost otrok na spletu in družabnih omrežjih', *Varuh človekovih pravic*, 3 October [Online]. Available at: <https://www.varuh-rs.si/sporocila-za-javnost/novica/zasebnost-otrok-na-spletu-in-druzabnih-omrezjih/> (Accessed: 18 November 2023).
- Varuh človekovih pravic (2019) 'Kdaj do zagovornika?', *Varuh človekovih pravic*, 21 August [Online]. Available at: <https://www.varuh-rs.si/sporocila-za-javnost/novica/kdaj-do-zagovornika/> (Accessed: 15 November 2023).

Children in Digital Age – Summary

Csenge HALÁSZ

The main task of the final chapter of this volume is to summarise the results of the research. To this end, the main conclusions of international and EU legislation are reviewed, followed by a summary of the children's rights that are very often violated on some online platforms.

Before doing so, however, it is worth starting the chapter with an overview of the internal regulatory models and different techniques that each global platform uses to better protect children's rights. The aim of this summary is to demonstrate that, in addition to effective regulation, the functioning of social networking sites needs to move towards the protection of children's rights in order to make a meaningful difference. The legal framework for the liability of digital service providers is beginning to emerge strongly, thanks also to European Union legislation, for example, but at the same time different platforms can make technological and internal regulatory changes that can greatly improve the framework for children's rights.

Having reviewed all these issues, the chapter concludes by outlining some of the regulatory and practical issues that may arise in the future. To assist students in their preparation, a glossary of definitions of relevant terms is included at the end of the volume.

1. Social Media Sites on the Road to Self-Regulation

The objective of the final chapter of this volume is to synthesise the valuable information contained in each chapter and draw conclusions. Before doing so, however, it is worth mentioning the recent trends that have been reflected in the strong self-regulation of each platform. Today, more and more online platforms are recognising the importance of protecting children's rights. The world's largest video-sharing platform, YouTube, for example, offers the possibility of using the so-called "*Restricted Mode*".

This effectively removes adult content from the user's channel.¹ This is also facilitated by the creation of the YouTube Kids interface, which also includes content specifically for children.² And for the slightly older age group, there is the option to set up “*supervised use*”, which essentially means that parents can determine the content their children can access.³ The largest video-sharing platform has come under criticism for the comments shared under each piece of audiovisual content. Under certain videos, negative comments can appear virtually every second, which can cause psychological problems for teenagers at a vulnerable age. In view of this, YouTube does not allow comments to be posted under videos in which children are involved.⁴ Reflecting the other side of the phenomenon, where it is often the youngest age group that is the most critical, from 2021 onwards, users of the video-sharing platform will not be able to comment on videos with children.⁵ Also welcome is the creation in 2018 of the Youth and Family Advisory Committee, which will regularly update the platform's family products and guidelines in consultation with experts on children's media content, child development, digital learning and digital citizenship. The Advisory Committee is composed of independent experts who provide sound advice to help ensure that the video-sharing portal protects children's rights as effectively as possible.⁶

From 2021 onwards, the global market leader Facebook has also made a number of changes to its interface and terms of use to help children's rights to be more effective. In particular, in addition to public content, messages sent in Messenger that depict or discuss child abuse or sexual exploitation can now be easily reported to the portal.⁷ The portal has also created a “*Parents' Conversations*” page aimed at educating parents to better understand some of the phenomena of the online world that has a very powerful impact on their children.⁸ The site also provides information material on preventing suicide among minors⁹, on sending and receiving intimate photos¹⁰, and contact details for law enforcement agencies.¹¹ However, the fact that these sites

1 See: <https://support.google.com/youtube/answer/174084?hl=hu&co=GENIE.Platform%3DDesktop> (Accessed: 23 June 2024).

2 See: <https://www.youtube.com/kids/> (Accessed: 25 June 2024).

3 See: <https://support.google.com/youtube/answer/10314940> (Accessed: 23 June 2024).

4 Orphanide, 2019.

5 See: <https://support.google.com/families/answer/10495678?hl=hu> (Accessed: 22 June 2024).

6 See: https://www.youtube.com/intl/ALL_hu/howyoutubeworks/our-commitments/fostering-child-safety/advisory-committee/ (Accessed: 23 June 2024).

7 See: <https://www.facebook.com/help/messenger-app/860170157674735> (Accessed: 23 June 2024).

8 For more on this see: https://www.facebook.com/safety/parents/conversations/what-parents-need-to-know-about-facebook-messenger-kids?locale=hu_HU (Accessed: 23 June 2024).

9 See: <https://about.meta.com/actions/safety/topics/wellbeing/suicideprevention> (Accessed: 23 June 2024).

10 See: <https://about.meta.com/actions/safety/topics/bullying-harassment/ncii> (Accessed: 23 June 2024).

11 See: <https://about.meta.com/actions/safety/audiences/law> (Accessed: 23 June 2024).

are only available in English is a shortcoming. Another new feature is the creation of an application called *MessengerKids*, which allows parents to create a chat account for their children, linked to their Facebook account, to interact with people of their choice, family members or friends.¹²

Another popular app among young people is Instagram, also owned by Meta, which has a key feature of focusing on images rather than text content, allowing users to essentially create their own personalised, yet publicly shared, photo album. Instagram is governed by the same guidelines and developments as Facebook, given that it is also run by the giant Meta. In addition, and for the sake of completeness, it should be noted that the European Union launched proceedings against the two social platforms in May 2024 under the mandate of the DSA Regulation, specifically to investigate the rights of children, who are considered a sensitive and vulnerable group.¹³ In this procedure, the EU Commission is examining the so-called “*rabbit hole*” effect, which is essentially the fact that social networking sites are highly addictive and considered to be high-risk platforms for the healthy development of children. The age detection mechanism of Meta and the adequacy of privacy settings for children will also be investigated.¹⁴

Among the actions taken by platforms to protect children’s rights, the most used and most addictive portal by young people is TikTok, which attracts users from all over the world with its short videos that can be scrolled continuously. Privacy and privacy concerns about the Chinese-developed portal date back practically to its birth, and its opaque data management and transmission practices, the proliferation of challenges that are spreading at an extraordinary speed and are very dangerous, have led to calls for stronger regulation and even a ban on the platform.¹⁵ To cite just one example, the governor of the US state of Utah has taken the initiative to ban the use of the app throughout the state, specifically on the grounds of protecting children’s rights. The state’s Attorney General has also supported the initiative, pointing out in a statement that the portal contains a number of misleading and untrue contents that adversely affect the healthy physical and psychological development of children and have a very harmful effect on the exercise of their individual rights. In her view, the constantly changing content, which reflects personal preferences, can create a strong addiction, even for the youngest age group.¹⁶ TikTok is not considered a leading social networking site in terms of self-regulation, but its Terms of Use contain provisions on minors.¹⁷ Accordingly, the platform does not allow any content that puts minors

12 See: <https://www.facebook.com/help/messenger-app/144677686167964> (Accessed: 18 July 2024).

13 European Commission, 2024b.

14 Ibid.

15 The United States and Canada have banned the use of the app on government devices, and European Commission staff are not allowed to use the TikTok platforms on their devices. See: Treasury Board of Canada Secretariat, 2023.

16 Gruyer, 2023.

17 See: <https://www.tiktok.com/community-guidelines/hu/youth-safety> (Accessed: 23 June 2024).

at risk of psychological, physical or developmental harm. If a user account violates these requirements, the TikTok platform will block that account and all accounts of the user concerned. Under the Terms of Use, TikTok will report cases of sexual abuse and exploitation of minors to the National Centre for Missing and Exploited Children. The portal also reports to the competent authorities when there is a concrete, credible and imminent threat to human life or a risk of serious bodily harm.¹⁸

The Terms of Use set by TikTok define the subject areas to which users under the age of eighteen have limited access. Examples include content related to eating disorders and body image disturbances, anabolic steroids promising drastic weight loss, and diets with alarmingly low calorie intake. Also restricted are videos showing dangerous challenges and activities that can be easily imitated and lead to physical injury. Videos with nudity, sexually suggestive or shocking and violent content are also covered by this restriction. A significant improvement is that videos showing gambling, alcohol and tobacco products are also restricted to users under the age of eighteen.¹⁹

To inform children and parents, TikTok has created a “*Minors’ Portal*”²⁰ and a “*Carers’ Guide*”.²¹ These platforms provide various information materials, with the aim of promoting children’s compliance with the law and providing parents and guardians with information on how the portal works and the risks that children may face when using the portal. In addition, as with the Meta innovation, TikTok also offers the possibility to create a family account, which means that parents can assign their child’s TikTok account to their own profile.²² In this way, the parent or guardian can make use of a number of settings that can have a positive impact on the protection of children’s rights and mitigate the harmful effects of the portal. In a significant step forward, the TikTok portal sets a default limit of one hour of screen time per day for teenagers aged between thirteen and seventeen, which a parent or guardian with a family account can change or monitor their child’s time on the app.²³ A similar regulatory approach will apply to notifications sent to the phones of young people aged between thirteen and eighteen. TikTok will automatically set time slots in the account of underage children where they will not receive notifications of newly shared content. For teens between the ages of thirteen and fifteen, the scheduled period is from 21:00 to 8:00. For teenagers aged 16 to 17, the scheduled period is from 22:00 to 8:00. Parents with a family account, however, have the option to set their child’s smartphone to “*silent mode*” within these factory-set periods.²⁴ Parents or guardians

18 Ibid.

19 Ibid.

20 See: <https://www.tiktok.com/safety/youth-portal?lang=hu> (Accessed: 4 August 2024).

21 See: <https://www.tiktok.com/safety/hu-hu/guardians-guide> (Accessed: 4 August 2024).

22 See also: <https://support.tiktok.com/hu/safety-hc/account-and-user-safety/user-safety#7> (Accessed: 4 August 2024).

23 See: <https://support.tiktok.com/hu/safety-hc/account-and-user-safety/user-safety#7> (Accessed: 4 August 2024).

24 Ibid.

also have the option to specify which users their child can receive direct messages from, or even turn off direct messaging on their child's account. By default, TikTok only allows users over the age of sixteen to send or receive direct messages through the application interface.²⁵

TikTok therefore tries to protect children's privacy rights through its internal rules and its various settings, but it is worth noting that TikTok, like Meta, was also the subject of a child protection procedure initiated by the Commission of the European Union in February 2024. The Commission is investigating whether TikTok has breached the DSA Regulation in the areas of protection of minors, transparency of advertising, access to data by researchers, and management of risks related to addictive design and harmful content.²⁶

The creation of internal rules, information materials and preferences by the social networking sites described above can clearly promote children's rights in the online space. However, it is important to note that, while these are laudable initiatives, they do not address all the issues that arise and most of them *can be 'circumvented'* with just a few clicks.

For example, most of the various internal rules do not reflect the very common phenomenon of an internet influencer parent promoting a product or service with their child on social media. Typical platforms include TikTok, Instagram and YouTube. The latter global video-sharing portal's policy is in some respects a step forward in that it does not allow commenting on videos in which a minor is involved. The two former platforms have not taken similar measures in this respect. In our view, it would also be worthwhile for the various global platforms to take stronger action against this phenomenon, given that its prevalence and the content of the videos can put children in a very vulnerable position.

Another major problem is that most of the various settings can be circumvented very easily by providing false information or by creating a profile that is not controlled by the parent, so that the settings made by the parent do not apply to the parent.

Overall, the initiatives of the self-regulatory models described above are certainly commendable in terms of protecting children's rights, especially with regard to the different information materials and settings. However, it should not be overlooked that the zero-price business model of the various global social networking sites also works in the interests of children: their personal data is processed and collected in order to make a profit, they are shown personalised advertisements and the platforms themselves can be considered highly addictive. However, in addition to the need for legal regulation, the individual platforms also have a huge responsibility to regulate their own operations in order to protect future generations.

25 See: <https://support.tiktok.com/hu/safety-hc/account-and-user-safety/user-safety#7> (Accessed: 4 August 2024).

26 European Commission, 2024a.

2. International Legal and EU Regulatory Environment – Summary And Conclusions

The digital environment has made interaction between children and children, and between children and adults, commonplace, and thus an inescapable fact of modern children's lives and well-being. Modern technology also enables children to create their own communities and to share attitudes and information about their daily lives within social networks. In addition, the fact that the prominent players in the digital space are privately owned and regulated in their own way is a significant factor.

In the course of the present research, a question of particular importance to be answered was: to what extent are the “*classic*” conventions and international regulations on children's rights suitable for protecting children's rights on the various Internet platforms, taking into account the dangers and specificities of the online world?

The “*flagship*” of these documents is essentially the UN Convention on the Rights of the Child (UNCRC)²⁷, which strongly declares a broad set of fundamental rights for children. The UNCRC contains a broad spectrum of children's rights, all of which are of paramount importance for the protection of our children's rights, but for the purposes of our topic it is obviously worth focusing on those that may be violated on the internet. For example, Article 16 of the Convention, which protects the privacy, reputation and honour of children, Article 17, which provides for children's right to mass media, and Article 18, which regulates the responsibilities of parents in relation to the upbringing of children, deserve special mention.²⁸

In addition to the UN Convention on Human Rights, there are other international conventions that greatly promote children's rights. Among these, the Second Optional Protocol to the UN Convention on the Rights of the Child (the “*Protocol*”) is the most prominent in protecting children in the digital world,²⁹ which seeks to protect children from commercial exploitation. In the age of the internet, where one of the most important features is fast and borderless communication, there are many ways in which children are sexually abused. Networking and communication about prostitution, pornography and trafficking of children for these reasons typically take place through various internet channels. States Parties that have accepted the Protocol are obliged to fully regulate and prohibit these acts in their criminal law, whether the relevant offences are committed domestically or internationally, and whether they are committed on an individual or organised basis. States Parties undertake to adopt laws and strengthen social policies and programmes to prevent the offences to which the Protocol applies. The Protocol aims to raise the standards to a higher level than those set out in Article 34 of the UN Convention on the Rights of the Child, thus

27 United Nations General Assembly, 1989.

28 Ibid.

29 Ibid.

strongly protecting children from exposure to various forms of criminal activity on the Internet.

It is a welcome trend that, in addition to the legislative products adopted under the auspices of the UN, there is also intense legislative activity at regional level. As regards the European region, the most important documents are the European Convention for the Protection of Human Rights and Fundamental Freedoms³⁰ (ECHR), the Convention on Cybercrime³¹ (Budapest Convention) and the European Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse³² (Lanzarote Convention).

Although all the conventions have been adopted by the Council of Europe and are therefore regional in nature, their impact is much broader than what can usually be expected from regional documents. The Budapest Convention, for example, offers effective legal responses to long-standing problems in the fight against cybercrime. In essence, it can be considered the first binding multinational treaty dealing with cybercrime and its provisions are therefore used as a model in many countries. The most valuable achievement of the Budapest Convention is the criminalisation of cybercrime and the creation of a system of cooperation between states against perpetrators.

The Lanzarote Convention is the first regional convention specifically aimed at protecting children from sexual violence. Adopted in 2007, it entered into force in 2010 and has been signed by all Council of Europe member states. Together with the Budapest Convention, this act is essentially a comprehensive protection of children's rights against the many threats of the digital world. By clearly defining the scope of offences against children and setting out guidelines for enforcement, the Lanzarote Convention provides a strong legal framework. It also provides strong rules and procedures for the protection of victims, which are important for children's mental health and self-confidence.

Summarising the international legal framework in this area, the UN Convention on the Rights of the Child is of particular importance in establishing the legal protection of children. It sets out the fundamental rights of children as a foundation that should guide them in the online and offline world. The various regional agreements, which in many cases also reflect the challenges of online platforms, are also a very welcome development.

The initial question of this sub-chapter can therefore be answered in the following way: the existence of multidisciplinary international conventions is essential for the protection of children's rights, as they set out the most basic standards. However, it is necessary to build on these norms, which must be done at regional and national level. Internet-specific legislation is essential to ensure effective protection of children's rights in the 21st century.

30 Council of Europe, 1950.

31 Council of Europe, 2001.

32 Council of Europe, 2007.

After reviewing the international legal documents, it is worth mentioning the conclusions of the European Union's regulatory trends. In this respect, a distinction can be made between binding and non-binding so-called *soft law* documents.

Among the latter, the EU Strategy on the Rights of the Child (2021)³³, which states that digital technologies offer children a wide range of opportunities for learning, entertainment and future employment, is worth highlighting. The strategy also draws attention to the impact of artificial intelligence on children's rights and safety. It supports the development of accessible ICT technologies for children with disabilities. It will also step up the fight against all forms of online child sexual abuse, for example by proposing legislation to oblige online service providers to detect and report child sexual abuse material. It also sets out concrete measures for Member States to improve access to digital tools, the internet, digital literacy and media literacy.

Another important document is the „*Digital Agenda 2030*”³⁴, which sets out the path for the Digital Decade in Europe, with child protection at the heart of this. The document points to the need to build a society in which children learn how to understand and navigate the myriad of information to which they are exposed online, through a wide range of digital skills. In addition, a people-centred, safe and open digital environment must also enable children's rights to be asserted. It is important to develop comprehensive digital principles that adequately protect children's rights in the online space.

The new strategy for a *Better Internet for Kids* (BIK+)³⁵, which aims to ensure that children's rights are protected in the new digital decade, has already been mentioned and is a priority. To this end, the document also sets out concrete actions for Member States and digital service providers. These include the development of effective age verification methods supported by Member States and digital education for children by adults, industry cooperation to develop reliable flagging programmes and to quickly assess and remove illegal content, and the development of products and services that promote children's right to expression.

Moving beyond soft law documents, it is worth mentioning the binding rules created by the European Union. Of these, the DSA Regulation³⁶, which responds to the challenges of global platforms in response to current social and technological challenges, and which also lays down provisions to protect children's rights, is of particular importance and deserves to be highlighted for the first time. To take one example, the protection of children is explicitly addressed in Recital 71 and Article 28. These provisions require platform providers to take appropriate and proportionate measures to protect minors. A further very strong step forward is that digital service providers are not allowed to display ads based on profiling and using personal data of the service user, if the service user is a minor.³⁷

33 European Commission, 2021b.

34 European Commission, 2021a.

35 European Commission, 2022.

36 European Parliament and the Council, 2022.

37 Ibid.

Also worth highlighting is the Audiovisual Media Services Directive (AVMS Directive)³⁸, as amended in 2018, which strengthens the protection of children from harmful content and inappropriate commercial communications. Examples of some of the relevant provisions of the Directive include Article 27, which requires Member States to ensure that access to audiovisual media services that are harmful to the physical, mental or moral development of minors is limited and appropriate to their level of maturity.³⁹ This can be ensured, for example, by measures such as the choice of the time of transmission or the use of age-rating devices proportionate to the harm that the programme may cause. The most harmful content should be subject to the most stringent measures. This provision also applies to audiovisual content on video-sharing portals.

Among the European Union legal documents protecting children's rights, the General Data Protection Regulation⁴⁰ (GDPR) adopted in 2016 and its recital 38, which states that children's personal data deserve special protection, deserve special protection. This special protection applies in particular to the use of data for marketing purposes and the creation of personality or user profiles, which are considered as common practice in the operation of global social platforms.

A relatively recent piece of EU legislation is the General Product Safety Regulation adopted by the Council in April 2023⁴¹, which declares that children have the right to safe products. It is important to note that online sales are also covered by the Regulation, so the legislation is quite forward-looking in terms of protecting children's rights.

Overall, the conclusion to be drawn from the European Union's regulation is that both mandatory and non-mandatory regulations are of great importance in creating a coherent and effective regulatory environment. This is supported by the fact that the European Commission has also launched child protection proceedings against TikTok, Instagram and Facebook, based on the DSA Regulation. Although the outcome of these proceedings is not yet known, it can be concluded that the EU legislation will allow for a more effective protection of children's rights on global internet platforms. In addition to legislation, there are also educational materials available in several languages, which can greatly help to inform children, parents and teachers and thus promote their compliance with the law.

3. Protecting Children's Rights Online – Lessons From a Central European Perspective

The aim of this sub-chapter is to synthesise the lessons learned from the country reports discussed in this volume to present a protection of children's rights that are

38 European Parliament and the Council, 2010.

39 Ibid.

40 European Parliament and the Council, 2016.

41 European Parliament and the Council, 2023.

typically at risk in different online platforms. The lessons from the different regulatory approaches of each country are thus brought together in one place.

3.1. Legal Framework for the Right to Privacy

The right to privacy, as a manifestation of the right to „*leave alone*”, a pre-eminent right involving a number of sub-rights, has become extremely sensitive and easily violated due to the effects of technological progress.

First of all, with regard to the Hungarian legal regulation, it can be noted that the regulation of the right to privacy is specific in that it is also provided for by a specific law, namely Act LIII of 2018 on the Protection of Privacy⁴², which states in its preamble that this right must be respected in both online and offline spaces. The Hungarian legislator does not contain any specific rules on the privacy of children, but the right to privacy is enshrined in the Civil Code and in the Fundamental Law, and is a right that everyone is entitled to.

The Polish Constitution gives everyone the legal right to protect their privacy, family life, honour and reputation.⁴³ The Constitution also guarantees the freedom and confidentiality of communication.⁴⁴ This is confirmed by the Polish Civil Code, which provides for the protection of this right. The protection of the image is ensured by the Copyright and Related Rights Act⁴⁵, the Personal Data Protection Act, which also contains a provision on the protection of children's images.⁴⁶

In Slovenia, the right to privacy and freedom of expression is protected at national level by the Constitution, which specifically protects the right to privacy.⁴⁷ It guarantees the inviolability of the physical and mental integrity of the human person, privacy and the rights of the individual, including the right to an image. When considering the right to privacy of children, Article 35 of the Constitution must be read in conjunction with Article 56 of the Constitution, which states that children enjoy human rights and fundamental freedoms in accordance with their age and maturity.

In Croatia, in addition to the relevant constitutional and civil law rules, the right to privacy is also guaranteed by the Civil Obligations Act, which states that in the event of a violation of privacy rights, the court may, if it finds that the gravity of the violation and the circumstances justify it, award fair monetary damages, regardless of whether or not there is compensation for material damage. Thus, the main means of legal protection in the country is also of a civil nature, but the Criminal Code of the State contains a provision on the protection of the right to privacy, as in other States, such as Hungary.⁴⁸

42 Act LIII of 2018 on the Protection of Privacy.

43 Article 47 of the Polish Constitution.

44 Ibid., Article 49.

45 Standardised text: Journal of Laws 2022 Item 2509.

46 Standardised text: 1781.

47 Article 35 of the Constitution of Slovenia.

48 Croatian Btk. Section XIV.

In the Czech Republic, the right to privacy is also regulated in a general way, by name in the Charter of Fundamental Rights, but, as in the previous legal systems, no specific provisions are laid down for children.⁴⁹

The right to privacy of children is not explicitly mentioned in the Family Code of the Republic of Serbia, but it is undoubtedly part of the rights of children. This follows from the Constitution of the State, which states that children are entitled to all human rights according to their age.⁵⁰

3.2. Regulation and Enforcement of Children's Freedom of Expression

In Hungary, freedom of expression is a fundamental right declared in the Fundamental Law⁵¹, which every person is entitled to. It is considered a communication mother right, which applies not only to oral and written communication, but also to communication in the online space.⁵² This freedom also extends to the right to information under the protection of freedom of expression, but importantly it cannot be considered an unlimited fundamental right.⁵³ Freedom of expression has traditionally been limited by child protection provisions. These standards are also regulated by the Hungarian Advertising Act, which states that advertising that is harmful to the physical, mental, moral or emotional development of children and minors is prohibited.⁵⁴ It is also important to note that these provisions should also apply to social networking sites.

Among other personal freedoms, the Polish Constitution guarantees everyone the freedom to express their opinions and to obtain and disseminate information.⁵⁵ As regards the right of children to express their views, Article 72(3) of the Constitution of the Republic of Poland, which establishes the constitutional criterion of the participation of the child in judicial proceedings, according to which the authorities and persons responsible for the child are obliged to listen to and take into account the views of the child when deciding on the child's rights, should also be highlighted.

The right to freedom of expression in the Slovenian legal system also has a constitutional basis.⁵⁶ The activities of the State Commissioner for Fundamental Rights, who has repeatedly stressed the need for the State to ensure that the views of the child are effectively heard in the various official proceedings, should also be highlighted. This commitment is enshrined in the laws governing the various procedures, including the

49 Act No 2/1993 Coll., Art.

50 Constitution of the Republic of Serbia Art.64/1.

51 Article IX of the Fundamental Law.

52 See: Freedom of speech [Online]. Available at: <https://ijoten.hu/szocikk/a-velemenynyilvanitas-szabadsaga> (Accessed: 2 August 2024).

53 Article IX(2)-(6) of the Fundamental Law.

54 Advertising Act § 8. In this section, the legislator also states that it is prohibited to make available to persons under the age of eighteen advertisements that depict sexuality for its own sake or that depict a minor in a dangerous or sexual situation.

55 Art. 54 of the Polish Constitution.

56 Art. 39 of the Constitution of Slovenia.

law on the placement of children with special needs.⁵⁷ Slovenia has also established a system of child representation to ensure that children are provided with adequate information.

In the Croatian legal system, Article 38 of the Constitution guarantees respect for freedom of expression. Considering that media literacy is one of the most important prerequisites for individuals to exercise their right to freedom of expression in the 21st century, the Croatian State takes various measures to promote media and digital literacy, which help children to access information and also set the framework for their freedom of expression.

In Serbia, in addition to the constitutional basis, the Law on Family Rights, which states that a child capable of forming his or her own opinion has the right to express it freely, is worthy of special mention in the area of children's freedom of expression. In this respect, the child must be provided with all the information he or she needs to form his or her opinion.⁵⁸

In Romania, there is a specific law on the protection and promotion of children's rights, which declares a basic set of rights for children to express their views and participate.⁵⁹ The article of the law on freedom of expression was amended in 2022 to include *expressis verbis* provisions on the online format, equating the online environment with traditional forms and channels of expression.

Article 26 of the Constitution of the Slovak Republic guarantees every individual the right to information and freedom of expression. Protection of the rights and moral development of minors is mentioned as one of the limits to this right, as in the legal systems of the other States under discussion. With regard to minors, the Slovak cybersecurity legislation contains specific provisions under which certain content that is harmful to the development of significant interests, such as the development of minors, may be blocked.

3.3 Children's Right to Access Information and Education in the Internet Age

The right to education, like the fundamental rights discussed earlier, is considered a constitutionally declared fundamental right in the Central European states, so the basis for state regulation in this respect is also provided by constitutional provisions.

The Polish state has recognised the need to raise digital competences to a high level in the context of developing children's right to education. Several state surveys have recently been carried out to assess the competence of the population in this area. Although the results of the 2023 IT competency test showed a higher average than in 2022 in the survey of digital competences of children and young people, primary school pupils scored only 46% and secondary school pupils only 43% on average.⁶⁰

57 Law on the placement of children with special educational needs, Uradni list RS, št. 58/11, 40/12 – ZUJF, 90/12, 41/17 – ZOPOPP in 200/20 – ZOOMTVI.

58 § 65/1 Serbia Law on Family Law.

59 Arts. 28-29 of Law 272/2004.

60 IT Fitness test, 2023.

In the light of these results, the Polish Council of Ministers Resolution No 24 of 21 February 2023 introduced the government initiative “Digital Competence Development Programme”⁶¹, which will be active until 2030. A number of objectives have been identified for school-age children, the most important of which are to prepare children and young people to operate safely, consciously and creatively in the information society and to create an environment conducive to the development of advanced digital competences and digital talents, taking into account the need to increase the participation of women and young girls in digital technology-related fields. The digital literacy agenda also takes into account statistics on the use of the internet and mobile devices by children under six and aims to engage pre-school children in the information society in a safe and aware way.

There is no specific legislation in the Slovenian legal system on children’s rights of access to information, which is essentially related to the right to education. In this respect, the activities of the Commissioner for Fundamental Rights should also be highlighted, as in the course of his activities he issues information materials on the rights of children and young people and provides support through online information, e-mail, telephone contact, personal assistance, postal services sent to the address of the institution, brochures, posters, leaflets and similar means. To facilitate information activities, the Slovenian police (among other institutions) provides a website specifically designed for children. This platform provides information on online safety and abuse.

Croatian legislation defines the right of children to education as a fundamental part of parental care. In relation to children’s rights of access to information in the digital environment, it is important to take into account the transposition of the AVMS Directive, which contains several provisions in relation to children’s digital rights, as it contains prohibitions to make content harmful to children’s development inaccessible.

Looking at the Serbian legal context, the right to education includes the obligation of the state, educational institutions and society to educate children *to become “digitally literate”*. Distance learning, introduced during the COVID-19 epidemic, presented many new challenges, with the “door” to cyberspace being opened wider than ever before, pupils creating numerous profiles, entering personal data on various platforms and spending more time online than ever before. In Serbia, a unified educational IT system has already been introduced in education, which has made some educational tasks more efficient, but some data management issues are raised by the way the system works.⁶²

One of the initiatives to be welcomed is the programme launched by the Slovak Republic called “Digital Support for Slovak Students (Digital Student)”. Under the nationwide project, different groups of students can apply for a grant of €350 to buy laptops or tablets with keyboards. The aim of the grant is to help primary and

61 Item 318 of the 2023 legal monitor.

62 Arts. 175/1.

secondary school students from socially disadvantaged backgrounds who would otherwise not have access to the tools they need to take advantage of the digital space. Access to Internet-connected devices also ensures access to information that is predominantly distributed and available online in the digital age.

3.4. Protection Against Abuse

Reading the pages of this volume, the clear conclusion is that, in addition to the many benefits offered by the digital world, there are also many dangers and negative effects of the various online spaces to which children are extremely exposed. It is therefore of the utmost importance that the individual legal systems in Central Europe provide adequate protection against abuse. Various civil, criminal and even administrative law instruments can be distinguished for this protection.

In Poland, for example, a number of offences typically involving children have been criminalised. One example is the crime of *grooming*, which is essentially sexual abuse committed by an offender who establishes a trusting, emotional relationship with the victim through an online platform, on the basis of which he or she commits the offence.

In Croatia, the right of children to protection against abuse in the digital environment, in particular in relation to the use of social networks and other forms of digital communication, is guaranteed primarily by the Criminal Code (CC). For example, the offence of harassment is mentioned, which also covers forms of harassment committed online.⁶³

In the Czech Republic, statistics show that 22% of pupils have experienced some form of cyberbullying. The Penal Code does not specifically mention forms of online sexual harassment, but the offence of sexual coercion, as defined in Article 186 of the Penal Code, also covers acts carried out through online platforms.⁶⁴

In terms of protection against certain abuses, it can be concluded that the institutions previously regulated in certain legal systems need to be applied to specific internet phenomena such as cyberbullying, grooming or sexting. In terms of the protection of children's rights, in all the Member States we have studied, considerable emphasis has been placed on protection against sexual exploitation and child pornography, which are also prohibited by international conventions to which the Central European States are party.

4. Concluding Thoughts

Overall, the protection of children's rights online in Central and Eastern Europe requires a comprehensive and integrated approach. The legal systems of the countries in this region are party to a number of multilateral international conventions and,

63 Art. 140 paras. 1–2.

64 Act No 40/2009 on the Criminal Code.

with the exception of Serbia, are members of the European Union, so these circumstances naturally have a strong impact on the legal systems under review, which obviously also protect children's rights within a state framework.

The issues addressed in this volume and in the “*Children in digital age*” course can be considered quite complex, taking into account the wide range of international and national regulations, as well as the functioning of global platforms and the self-regulatory models they use. However, it is reasonable to conclude from the research that the States studied have clearly recognised the obligation, based on social and technological changes, to provide stronger protection of children's rights on the Internet. The statistics are undisputed: young people spend a significant part of their day online, enjoying the benefits of the ‘*brave new digital world*’. However, those under the age of eighteen are particularly vulnerable to the highly addictive nature of these platforms. On the other hand, new phenomena such as cyberbullying, grooming, sharenting and sexting are associated with them. Protection against these phenomena can of course be achieved through the law. However, the research has shown that the majority of the countries surveyed are still trying to respond to these new phenomena by using the concepts and systems of the offline world, rather than creating new rules. The situation is similar for the protection of children's rights such as the right to privacy, the right to a portrait, freedom of expression, the right to education and the right of access to information, which are recognised by the States for all their citizens, but where there are few specific rules for children or for the online world. However, it is worth highlighting that public institutions such as ministries, data protection authorities, ombudsmen, NGOs and public child welfare institutions, which are responsible for these areas, have produced a range of educational materials to help inform children, parents and teachers. In this way, the States are essentially recognising the importance of education, which is essential for the protection of children's rights, since on the one hand it is more effective to prevent a violation than to remedy it afterwards. On the other hand, children need to be informed as widely as possible about the dangers they face in the online world and who they can turn to if they are victims of harassment, for example, or if their personal data or even their image is misused.

Which online challenges are the most likely to threaten children's rights in the future? To give just a few examples, these could include potential mental health issues, given that the long-term psychological effects of different internet platforms on the youngest internet users are not yet known. The effects of the so-called digital footprint could also be a long-term problem. Children's digital footprints - the sum of the traces they leave online - may well affect their future opportunities, including their job prospects and social contacts. So the biggest challenge is how to protect children's digital footprints from becoming fully public and how to educate them about conscious and responsible online behaviour. A third challenge is the growing presence of artificial intelligence (AI) and automated decision-making in social media, including content moderation and personalisation of the user experience. However, AI-based systems often do not take into account the specific needs and sensitivities of children. In the

future, it will be an important challenge to ensure that these systems do not violate children's rights and that appropriate regulation and oversight mechanisms are in place to ensure that their rights are protected.

These challenges echo the words of Melissa Müller, which we have chosen as the motto of our book. The pervasive system of global social networks is a clear threat to children's rights. The key to *their 'escape'* from the clutches of the '*giant, greedy marketing machine*' is twofold: on the one hand, they need to understand this new world of media, to see the disadvantages clearly and to use the advantages. On the other hand, they need a legal environment that gives them the fullest possible protection. The Central European countries are making great progress in this respect, but it is time to incorporate some specific elements into their legal systems.

Bibliography

- Council of Europe (1950) European Convention for the Protection of Human Rights and Fundamental Freedoms, *Council of Europe Treaty Series*, No. 005 [Online]. Available at: https://prd-echr.coe.int/documents/d/echr/Convention_HUN (Accessed: 6 August 2024).
- Council of Europe (2001) ‘Convention on Cybercrime (ETS No. 185)’, *Council of Europe Treaty Series No. 201* [Online]. Available at: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (Accessed: 6 August 2024).
- Council of Europe (2007) ‘Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse’ [Online]. Available at: <https://rm.coe.int/168046e1d2> (Accessed: 3 August 2024).
- European Commission (2021a) ‘Digital compass to 2030: the European way to deliver the digital decade, COM(2021)118 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021DC0118> (Accessed: 5 August 2024).
- European Commission (2021b) ‘The EU Strategy on the Rights of the Child and the European Children’s Guarantee, COM(2021)142 final’ [Online]. Available at: <https://eur-lex.europa.eu/HU/legal-content/summary/eu-strategy-on-the-rights-of-the-child-and-the-european-child-guarantee.html> (Accessed: 5 August 2024).
- European Commission (2022) ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Decade For Children And Youth: The New European Strategy For A Better Internet For Kids (BIK+) COM(2022)212 final’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0212> (Accessed: 4 August 2024).
- European Commission (2024a) ‘Commission opens formal proceedings against TikTok under the Digital Services Act’, *ec.europa.eu*, 19 February [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_24_926 (Accessed: 4 August 2024).
- European Commission (2024b) ‘Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram’, *ec.europa.eu*, 16 May [Online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2664 (Accessed: 2 August 2024).
- European Parliament, European Council (2010) ‘Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)’ [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013> (Accessed: 2 August 2024).

- European Parliament, European 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/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (Accessed: 2 August 2024).
- European Parliament, European Council (2022) 'Regulation (EU) 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' [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065> (Accessed: 2 August 2024).
- European Parliament, European Council (2023) 'Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and of the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC' [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0988> (Accessed: 2 August 2024).
- Gruver, M. (2023) 'Utah sues TikTok, alleging it lures children into addictive and destructive social media habits, *apnews.com*, 10 October [Online] Available at: <https://apnews.com/article/utah-tiktok-lawsuit-social-media-children-2e8ab3cfc92b58224ed9be98394278e0> (Accessed: 22 June 2024).
- Orphanides, K.G. (2019) 'On YouTube, a network of paedophiles is hiding in plain sight', *Wired*, 28 February [Online]. Available at: <https://www.wired.com/story/youtube-pedophile-videos-advertising/> (Accessed: 23 June 2024).
- Treasury Board of Canada Secretariat (2023) 'Statement by Minister Fortier announcing a ban on the use of TikTok on government mobile devices', *Government of Canada*, 27 February [Online] Available at: <https://www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html> (Accessed: 27 July 2024).
- United Nations (1989) 'Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty' [Online]. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/second-optional-protocol-international-covenant-civil-and> (Accessed: 6 August 2024).
- United Nations General Assembly (1989) 'Convention on the Rights of the Child, New York, 20 November, General Assembly resolution 44/25' [Online]. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> (Accessed: 6 August 2024).

Collection of terms

A ZERO-PRICE BUSINESS MODEL: The essence of this model is to attract consumers (often children) to the site by sharing and constantly updating content on the site, and collecting data on their activity. This activity obviously has a strong impact on the right to the protection of personal data, since the social platform collects information on the pages visited by users, their preferences, the content they like and share.

CHILD: According to Article 1 of the Convention on the Rights of the Child, signed in New York on 20 November 1989, like various international legal instruments, a child is a person who has not attained the age of 18 years, unless he or she has attained majority under the law applicable to him or her. The rights of persons under the age of 18 may be regulated differently in different national legal systems, for example in relation to capacity.

CONSCIOUS INTERNET USE: Means using the internet in a thoughtful, intentional and responsible way. It involves controlling the consumption of online content and online activities to ensure that they are consistent with one's personal values, goals and well-being. The concept is of particular relevance to children's use of the Internet, of which appropriate education is a crucial element.

CYBERBULLING: An activity in which one person or group intentionally and repeatedly harasses or intimidates another through online platforms such as social media, text messages, or emails. This behaviour can manifest itself in sending abusive messages, posting malicious comments, sharing humiliating pictures or videos, and engaging in other manipulative online activities.

E-PARENTING: The term refers to how parents manage and control technology, especially the internet and digital devices, when they are in contact with their children. There can be many different aspects of e-parenting and the aim is generally to help parents help their children develop a safe, responsible and positive online presence.

FILTER BUBBLE: A phenomenon that occurs when an individual or group has access only to information or opinions that confirm or reinforce their pre-existing views or belief systems. Social media can often contribute to opinion bubbles, as algorithms tend to display content that matches an individual's preferences, and thus limit access to information in terms of diversity or opposing views.

FOMO: Acronym for Fear of Missing Out. Meaning: fear of missing out.

GROOMING: Grooming is when an adult gets close to a child in order to get him or her to engage in some kind of sexual activity.

SEXTING: The sending of erotic, sexual text messages, pictures and videos of this nature by smartphone (less often by computer).

SHARENTING: A phenomenon whereby parents or relatives post large amounts of detailed information about the child concerned in the form of photographs, videos or text messages on social media, in violation of the child's right to privacy.

SMART DEVICE: Various devices and appliances that have an IP address and are able to send and receive data over the internet.

SOCIAL MEDIA: In a general sense, services (websites and applications) that provide a framework that, once registered, allows users to become part of an online social network, where they can access, create and share content. However, it is not possible to give an exact definition of social networking sites, given their diversity and their constant evolution. Moreover, social networking sites can be grouped into several categories. For example, there are classic social networks such as Facebook, chat services such as messenger, video-sharing portals such as TikTok and YouTube, and thematic applications.

