Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
75
1949 - 2024
CONSEIL DE L'EUROPE

Doc. 15954
27 March 2024

The protection of children against online violence

Report[1]
Committee on Social Affairs, Health and Sustainable Development
Rapporteur: Mr Joseph O'REILLY, Ireland, Group of the European People's Party

Summary

It is urgent to protect children from violence in the digital environment in view of growing dangers on the internet and new forms of online violence. Creating a safe environment and minimising the risk of harm are essential to protect children online. While ensuring a balance between the protection of children and their freedom of expression and other competing rights, the best interests of the child should prevail in the development and implementation of any measure or policy.

The report recommends establishing a comprehensive legal framework to protect children in the digital environment. This framework should include effective age verification obligations on websites providing goods and content which are not intended for children, and which would incur similar obligations in the offline world; specific measures to protect young children from premature exposure to the digital environment given their vulnerability to violent or sexual content; school-based educational programmes; the ban on harmful deepfakes and their removal from digital platforms.

The Committee of Ministers of the Council of Europe should consider the dangers posed by the internet to children, in particular in its work on the draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law and on age-appropriate comprehensive sexuality education. It should also strengthen its co-operation with digital industry stakeholders.

1. Reference to committee: Doc. 15383, Reference 4614 of 30 September 2021.

Contents **Page**

A. Preliminary draft resolution[2]

1. The Parliamentary Assembly stresses the urgent need to protect children from violence in the digital environment, especially in view of growing dangers on the internet and new forms of online violence.

2. Children are increasingly exposed to various forms of online violence, sometimes from an early age. The physical and psychological repercussions are often devastating. Increased use of the internet and digital tools, particularly during the Covid-19 pandemic and lockdowns, has led to children being overexposed to age-inappropriate content and behaviour. Smartphones have undoubtedly opened up a new avenue for personal development online, but they are also a potential source of violence.

3. Creating a safe environment and minimising the risk of harm are essential to protect children online. Mindful of the difficulty of reconciling the protection of children and their freedom of expression and other competing rights, the Assembly reiterates that the best interests of the child must prevail in the development and implementation of any measure or policy.

4. The Assembly therefore calls on member States to establish a comprehensive legal framework that protects children in the digital environment by applying an integrated and balanced approach to reduce exposure to harm online while not infringing on children's opportunities to benefit from the internet. In particular, it asks the member States to take the following steps to protect children:

4.1. as a minimum standard, impose effective age verification obligations on websites, particularly on sites providing goods and content which are not intended for children, and which would incur similar obligations in the offline world;

4.2. involve and raise awareness of parents and caregivers, who often lack the knowledge and support to detect online exploitation, abuse and violence, and empower them to deal with it;

4.3. take specific measures to protect young children from premature exposure to the digital environment given their vulnerability to, *inter alia*, violent or sexual content and the limited benefits of digital tools with respect to their particular physical, physiological, social and stimulation needs;

4.4. in order to prevent child sexual abuse material and punish perpetrators, set up hash databases supplemented with the due cybersecurity measures with a view to expediting actions to identify and locate children subjected to sexual exploitation or abuse; remove or restrict access to such content; apprehend perpetrators; and provide child victims with the necessary psychological support and rehabilitative care;

4.5. implement school-based educational programmes, in particular to promote peer-to-peer interactions and parental involvement;

4.6. in such programmes, provide children and young people with training on assertiveness, empathy, problem solving, emotion management and help seeking;

4.7. implement comprehensive sexuality education that covers the issues of online dating and relationships in depth and aims to counter portrayals of violence in sexual relationships and homophobic bullying;

4.8. run information and awareness-raising campaigns on harmful deepfakes, including those of a pornographic nature; ban deepfakes and ensure their removal from digital platforms.

5. The Assembly recommends that member States work closely with stakeholders in the technology industry in order to:

5.1. improve the development of policies and regulatory frameworks and facilitate their appropriation and implementation by the technology industry;

5.2. increase the accountability and responsibility of stakeholders in the technology industry to protect child users, including by requiring them to provide assistance to law enforcement authorities in terms of technical support and equipment to facilitate the identification of perpetrators of crimes against children and the collection of evidence required for criminal proceedings;

5.3. develop and implement policies that address cyberbullying, harassment and incitement to hatred and violence in the digital environment, including clear information on unacceptable behaviour, reporting mechanisms and the importance of support for children affected by such conduct;

2. Draft resolution adopted unanimously by the committee on 25 March 2024.

5.4. integrate safety and privacy in the design and by default, while taking into account children's right to protection from violence online, as guiding principles for the features and functionalities of products and services intended for or used by children.

6. In line of the latest edition of the European Day on the Protection of Children against Sexual Exploitation and Sexual Abuse on 18 November 2023, the Assembly is convinced of the importance of learning from victims and survivors of childhood sexual violence in order to develop effective policies based on real-life experiences. It recommends that member States listen to victims of childhood online violence, taking all necessary precautions, when drawing up measures and policies to prevent, protect against and combat online violence.

7. The Assembly notes the importance of international and cross-border co-operation in protecting children from online violence and calls for as many countries as possible around the world to accede to the relevant treaties and effective mechanisms that already exist. In this respect, it calls for:

7.1. observer States and St ates whose parliaments enjoy observer or partner for democracy status with the Assembly to accede to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, Lanzarote Convention);

7.2. member and observer States of the Council of Europe, and States whose parliaments enjoy observer or partner for democracy status with the Assembly that have not yet done so to accede to the Convention on Cybercrime (ETS No. 185, Budapest Convention);

7.3. Council of Europe member States that have not yet done so to join INTERPOL and its International Child Sexual Exploitation Database to exchange information on child sexual abuse cases.

8. The Assembly commends the Committee of the Parties to the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Committee) for its work on the second monitoring round (2017-2022) on the implementation of the Lanzarote Convention, focusing on the protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs) and addressing the challenges raised by child self-generated sexual images and/or videos. It invites the States Parties to the Lanzarote Convention to pursue their work on children and emerging technologies, in particular artificial intelligence and the virtual world, in greater depth, taking into consideration new risks for children, including those linked to deepfakes of a sexual or pornographic nature.

9. The Assembly is determined to further examine the issue of "violent pornography", including pornography available online, taking into account the specific problem of children being exposed to such content.

B. Preliminary draft recommendation[3]

1. The Parliamentary Assembly refers to its Resolution … (2024) "The protection of children against online violence". It invites the Committee of Ministers to take into due consideration, in its work, the dangers posed by the internet to children, who are more exposed to violence and new forms of violence in the online environment, in particular by:

1.1. considering and incorporating the best interests of the child in the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, including the protection of children's human rights from the dangers of artificial intelligence;

1.2. taking online violence into account in its feasibility study on age-appropriate comprehensive sexuality education;

1.3. strengthening international co-operation with relevant organisations, including the European Commission and relevant European Union agencies such as Europol and the European Union Agency for Fundamental Rights, and INTERPOL, with a view to focusing attention on the protection of children's human rights and the best interests of the child.

2. The Assembly calls on the Committee of Ministers to strengthen co-operation with digital industry stakeholders in order to find adaptable and sustainable solutions to protect children from online violence, including by:

2.1. as a first step, assessing the reliability of age verification tools, depending on the content and the age of child users;

2.2. providing children and parents with tools to raise awareness of the dangers of the internet;

2.3. making online tools available to enable easy reporting of incidents of online violence, and providing help and support, particularly psychological care, for child victims.

3. Draft recommendation adopted unanimously by the committee on 25 March 2024

C. Explanatory memorandum by Mr Joseph O'Reilly, rapporteur

1. Introduction

1. The internet presents tremendous opportunities for children as a source of knowledge, a tool for communication and a springboard for creativity. However, with these opportunities come serious risks to children's safety and well-being. This is the reason why the Committee on Social Affairs, Health and Sustainable Development (hereinafter, the committee) decided to table a motion for a resolution concerning the protection of children while using the internet,[4] at the initiative of a group of Irish children involved in the committee's child participation pilot project 2020-2022.

2. Both the Parliamentary Assembly[5] and the Committee of Ministers[6] of the Council of Europe have already addressed the protection of children on the internet. Conscious that the use of the internet can generate risks, including violence, exploitation and abuse,[7] and that these dangers have increased during the Covid-19 pandemic and lockdowns, we need to revisit the issue again. We need to take into consideration not only the latest risks and threats for children in the online environment, but also children's rights and expectations. We need to look at the impact of the most recent developments in technology, of children's practices online and of the legal framework. Today – especially since the Covid-19 pandemic and the transition of many educational and social activities online – children are autonomous actors on the internet. They are not only users and observers of content and platforms, but have become producers, staging themselves on social networks and increasingly curating and sharing their image and personal data.

3. It is of crucial importance to continue to empower children as online actors, enabling them to access information, education, socialisation and to share their opinions, while improving and enforcing a framework that will protect them against exposure to harmful content and behaviours. Prevention and early detection of illegal, abusive or harmful material must be reinforced. Restrictions on publications by children is a measure which could be considered, when it is in the best interest of the child, taking into account the individual situation and capacities. However, such restrictions on the freedom of expression and privacy of the child should always comply with the conditions laid down by the European Convention on Human Rights (ETS No. 5), implying, among other considerations, that they should have an accessible and foreseeable legal basis and may not be arbitrarily imposed.

4. While some of the risks remain similar or identical to those previously identified, exposure to the internet has increased exponentially. Our societies, first and foremost children and young people, have become accustomed to the use of the internet as an almost seamless continuation of their offline lives. With this increased internet traffic has come an increase in the volume of reported abuse. Some 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online.[8] The age at which children are first exposed to sexually explicit content seems to be dropping by a full year every two years.[9] New emerging technologies such as generative artificial intelligence (AI) pose new risks for the safety of children online, as do harmful deepfakes, including pornographic deepfakes.[10] New trends are emerging, such as financial sexual extortion, while threats like online grooming or children's "self-generated" sexual material continue to grow.[11] A 2023 report by the Internet Watch Foundation points to the worrying new phenomenon of AI being abused to create child sexual abuse imagery.[12] Politicians must analyse this phenomenon and take it into consideration without delay.

---

4. Doc. 15383, Motion for a resolution, "Right of the child to protection while using the internet". The motion was referred to the committee on Social Affairs, Health and Sustainable Development for report and I was appointed rapporteur on 25 April 2022. A public hearing was held in Strasbourg on 26 January 2023, AS/Soc (2023) PV01add2.
5. See for instance: Recommendation 1882 (2009) "The promotion of Internet and online media services appropriate for minors", Resolution 1834 (2011) and Recommendation 1980 (2011) "Combating 'child abuse images' through committed, transversal and internationally co-ordinated action", Resolution 2001 (2014) "Violence in and through the media", Resolution 2144 (2017) and Recommendation 2098 (2017) "Ending cyberdiscrimination and online hate", Resolution 2314 (2019) "Media education in the new media environment", Resolution 2429 (2022) and Recommendation 2225 (2022) "For an assessment of the means and provisions to combat children's exposure to pornographic content".
6. See: Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment (28 April 2021); Council of Europe Strategy for the Rights of the Child (2022-2027): "Children's Rights in Action: from continuous implementation to joint innovation", Strategic objective and action No.3 (Access to and safe use of technologies for all children).
7. See the Preamble of Recommendation CM/Rec(2018)7, op. cit.
8. UNICEF, "Protecting children online".
9. We Protect Global Alliance, "Global threat assessment 2021".
10. See Resolution 2498 (2023), "Youth and the media".

2. The dimension of risks for children online and the need to empower children

5. The internet presents many possibilities for children in terms of socialising, leisure, shopping and education, including information and online teaching. Children are not only passive recipients of information, but engaged and active participants in the online world.[13] It is estimated that one in three internet users is under 18 years old.[14] International Telecommunication Union statistics show that three-quarters of young people aged between 15 and 24 years worldwide use the internet, while the figure is 98% in Europe.[15] This shift to the online world has been intensified due to the Covid-19 pandemic during which sometimes the only social interaction possible took place via online platforms.[16] At the same time, children are more vulnerable than adults and therefore more likely to be abused or otherwise harmed online.

6. As it is not always immediately visible or apparent when or how children's rights are violated in the digital age, it is crucial to get their point of view on the matter in order to fully comprehend the dangers and challenges they face while using the internet.[17] In my opinion, the solution to the problem can only be reached by applying a child-centred approach. By talking to children, we are better able to understand not only the negative experiences they face in accessing the internet, but also the opportunities they enjoy and the skills and competences they acquire by engaging in online activities. From this starting point, we can better appreciate and analyse children's exposure to online risks and possible harms, and the role of their parents as mediators and sources of support. Recalling Baroness Massey's report on child participation,[18] I believe that children's own voices and experiences should be at the centre of policy development, legislative reform and programme and service delivery, for the sake of the children's best interests. I would also like to mention an interesting piece of research drawing on conversations with young survivors of online violence called "Disrupting harm – Conversations with young survivors",[19] which is a good example of the relevance of involving children in policy making. In line with the latest edition of the European Day on the Protection of Children against Sexual Exploitation and Sexual Abuse on 18 November 2023, I am convinced of the importance of learning from victims and survivors of childhood sexual violence in order to develop effective policies based on real-life experiences. I therefore propose that the member States listen and take into account the testimonies and suggestions of victims of childhood online violence when drawing up measures and policies to prevent, protect against and combat online violence.

7. The speed of technological innovation requires us to assess the risks that it may pose to children's mental and physical well-being, as well as their right to protection. New and unforeseeable risks may develop quickly and can threaten children's safety before their parents, teachers or caregivers are aware of such risks.[20] The identification of risks is important in order to build effective policies. Online safety risks have been classified in four categories: content, contact, conduct and commerce (sometimes referred to as contract). These are known as the 4Cs of online safety.[21]

8. First, content risks which arise as the child is exposed to pre-produced media content that may have a negative effect, such as pornographic or racist content. Second, contact risks which children can face when interacting with other users online who put them at risk – for instance grooming or exploitation. Third, conduct risks which occur as children participate in peer-to-peer interactions which can be harmful such as cyberbullying or incitement to self-harm, sharing or receiving nude and semi-nude images and viewing or sending pornography. Lastly, contract risks which concern children agreeing to unwanted, exploitative or age-inappropriate contracts, like online gambling and inappropriate advertising.

---

11. We Protect Global Alliance, "Global threat assessment 2023".
12. Report on "Child sexual abuse material (CSAM) generated by artificial intelligence (AI)", Internet Watch Foundation, 2023.
13. UN Special Representative of the Secretary-General on Violence Against Children, "Releasing children's potential and minimizing risks – ICTs, the Internet and violence against children".
14. UNICEF, "One in Three: Internet Governance and Children's Rights".
15. International Telecommunication Union, "Youth Internet Use", 2002.
16. "Responsible Innovation in Technology for Children", Daniel Kardefelt Winther, Innocenti Research Report, UNICEF Office of Research – Innocenti, Florence, 2022.
17. UNICEF, "Global Kids Online Comparative Report", Innocenti Research Report, 2019.
18. Doc. 15435, Resolution 2414 (2022) and Recommendation 2218 (2022) "The right to be heard – child participation: a foundation for democratic societies".
19. Report on "Disrupting harm – Conversations with young survivors, about online child sexual exploitation and abuse", ECPAT International 2022, Global Partnership to end violence against children.
20. "Handbook for policy makers on the rights of the child in the digital environment", Council of Europe, 2020.
21. Livingstone, S. and Stoilova, M. (2021), "The 4Cs: classifying online risk to children".

9. According to meta-analyses of international studies on the different forms of violence against children online recently highlighted in a survey by the World Health Organisation (WHO), 8% of adolescents had had a self-made sexual image forwarded without consent, while 11.5% of survey participants had received unwanted online sexual solicitations and 15% of children reported cyberbullying and victimisation.[22] Moreover, other research comparing different regions also indicates that children are exposed to a worrying level of online content relating to suicide and self-harm, sexual or violent content and hate speech, among others.[23] A French study showed that children are increasingly exposed to pornography. 63 % of boys and 37 % of girls aged 15 to 17 years have watched content on such a website at least once.[24] The pandemic has further aggravated the exposure of children to pornography[25] as well as child sexual abuse images.[26]

10. The International Child Sexual Exploitation Database (ICSE), INTERPOL's technical platform, has helped identify 37 900 child victims of sexual exploitation worldwide so far and 16 533 perpetrators, often with more than one victim.[27] On average, 15 victims are identified every day.[28] During the pandemic, there was a spike in child sexual exploitation and abuse online: sexual abuse online of children went up by 50% in some European countries.[29]

11. However, the data available is not exhaustive and gaps remain in our understanding of the full extent of violence against children online. This is also because this type of violence remains largely hidden because of fear, shame, stigma and a lack of support services. Less than half of the children exposed to violence tell anyone.[30] The data can, moreover, often only indicate the extent of risks children are exposed to online and not the actual harm caused. This underlines the need to create child-friendly support systems.

12. Violence against children online also constitutes a significant public health issue. The sexual abuse of children poses a major risk of physical, mental and social health problems later in life such as depression, anxiety, post-traumatic stress disorder, substance abuse and other health risk behaviours. Even after the abuse, victims often live in fear of the use or resurfacing of images. Cyberbullying can lead to physical health problems including insomnia, gastro-intestinal issues and chronic pain as well as to mental health problems and the increase of health risk behaviours, for instance sexual risk-taking. Let me just recall the consequences of violence in all its forms on children. Child abuse and exploitation have been associated with poor academic outcomes, the risk of serious social consequences on subsequent relationships and problems at work.[31] Consequently, the opportunities for the rest of the child's life are impacted and the risk of affecting the next generation with the survived trauma is greatly increased.[32]

13. As children interviewed for a report stated, safety is fundamental for their well-being online. In their view, safety means the absence of danger and a feeling of being protected.[33] Measures to protect children online must be specifically targeted at the problems. Overly restrictive measures for protecting children from exposure to danger online come with the downside of reducing their online opportunities and limiting the development of their digital skills. In our societies today, it is clear that the internet plays a crucial role in the daily life of children and the opportunities that come with this should not be denied. It is usually the content and contact with others which create an unsafe environment, not the activities as such. The answer is therefore to regulate the activities so as to create a safe environment and minimise the potential for harm. This all leads to one goal: children need to be (more) empowered online.

---

22. WHO, "What works to prevent violence against children online?", 24 November 2022.
23. UNICEF, "Global Kids Online Comparative Report".
24. "Les adolescents et le porno: vers une "Génération Youporn"?", Sondage IFOP for the Observatoire de la parentalité et de l'éducation numérique.
25. See Resolution 2429 (2022) and Recommendation 2225 (2022) "For an assessment of the means and provisions to combat children's exposure to pornographic content".
26. OSCE and UN Women, "Addressing emerging human trafficking trends and consequences of the COVID-19 pandemic".
27. Public hearing on the "Right of the child to protection while using the internet", Strasbourg, 26 January 2023, AS/Soc (2023) PV01add2.
28. INTERPOL, International Child Sexual Exploitation Database, data as at 31 December 2023.
29. We Protect Global Alliance, "Global Threat Assessment 2021".
30. WHO, "Violence against children online – What health systems and health care providers can do", 30 June 2022.
31. *Ibidem*. See also Resolution 2521 (2023) and Recommendation 2263 (2023) "Mental health and well-being of children and young adults", and Resolution 2520 (2023) and Recommendation 2262 (2023) "Preventing addictive behaviours in children".
32. WHO, "Global plan of action to strengthen the role of the health system within a national multisectoral response to address interpersonal violence, in particular against women and girls, and against children" (2016).
33. UNICEF, "Responsible Innovation in Technology for Children", *op. cit*.

14. There is obviously an urgent need for a comprehensive legal framework that protects children. States should take more action to protect the rights of children, by applying an integrated and balanced approach to reduce exposure to harm online while not infringing on children's opportunities to benefit from the internet.[34] In order to achieve the most effective protection, States need to bring on board parents and caregivers, who often lack sufficient knowledge or support in detecting and responding to exploitation, abuse and violence online.[35] They should also work closely with the technology sector in developing and implementing policies and frameworks, thus increasing their responsibility and accountability in protecting users.

15. I also believe that sexuality education should include measures to help children stay safe online. A WHO report highlights the importance of implementing educational programmes for children and parents to prevent online violence. The report states that comprehensive forms of sex education can reduce physical and sexual aggression – in particular homophobic bullying, dating and partner violence. The effectiveness of sex education has been confirmed in all countries.[36] The Committee of Experts on the prevention of violence (ENF-VAE) should consider the online aspect of violence against children in its ongoing feasibility study on age-appropriate comprehensive sexuality education.[37]

3. The importance of technology and the role of the technology sector in protecting children online

16. Technology offers endless opportunities to children, not least in the field of education. It can promote their empowerment and participation, and these positive aspects should always be borne in mind when developing measures to mitigate the risks. Indeed, technology can also play a powerful role in ensuring and enhancing the protection of vulnerable children, who can use online services to access information from institutions, seek advice from child helplines or report incidents and request assistance.

17. It is therefore important to make children aware of these possibilities as well as of the dangers. Children are far from passive when it comes to their online safety. Research has shown they are capable of developing strategies to deal with negative experiences, such as blocking insulting contacts and withholding personal information; finding details about safety advice online; changing privacy settings on a social networking profile; comparing websites to judge their quality or block spam.[38]

18. In order to ensure a safe environment online, it is crucial that the technology used is child-friendly. This encompasses all steps, from the design of websites to the provision of adequate reporting mechanisms. Whenever tech companies create digital services or products accessible to children, these should be designed to meet the needs and uphold the best interests and rights of children.[39] I therefore recommend involving children from the first stage of designing the platform. Furthermore, member States, if they have not done so already, should promote and provide incentives for businesses in the technology sector to integrate safety and privacy in the design and by default as guiding principles for the features and functionalities of products and services intended to or used by children.

19. This underlines the pivotal role of the technology industry in ensuring online safety and protection for children. Tech companies are responsible for their websites and their content, especially when they make huge efforts to attract children towards their products and services. They must therefore be held accountable.[40] This calls for close collaboration between the State and the technology sector in identifying solutions in a fast-moving environment, and for the imposition of legal obligations on tech companies to put in place adequate measures to protect children and prevent misuse of their services.

20. A study asking children about the prerequisites for a safe environment online confirmed that appropriate safeguards are crucial, for instance by requiring age checks, limiting possible contact with strangers and ensuring parental control, but all while continuing to ensure the digital empowerment of children.[41] Parental guidance and control are not efficient enough to be the primary safeguard mechanism, especially as the danger arises from the websites themselves.

---

34. UNICEF, "Global Kids Online Comparative Report".
35. UN, "Releasing Children's Potential and Minimizing Risks – ICTs, the Internet and Violence against Children", *op. cit*.
36. WHO, "What works to prevent violence against children online?", *op. cit*.
37. Committee of Experts on the prevention of violence (ENF-VAE).
38. S. Livingstone, L. Haddon, A. Görzig and K. Ólafsson, "Risks and Safety on the Internet: The perspective of European children". LSE and EU Kids Online.
39. Council of Europe, Strategy for the Rights of the Child (2022-2027).
40. Public hearing on the "Right of the child to protection while using the internet", *op. cit*.
41. UNICEF, "Responsible Innovation in Technology for Children", op. cit.

21. The first step to protect children online while protecting the right to internet access is to introduce child age verification tools. These tools are based on the mass collection of personal data, which constitutes a problem in itself, and often prove very easy to circumvent, for instance by simply confirming an e-mail. A study shows that around 44% of the children aged from 11 to 18 years have lied about their age online.[42] Proper and appropriate age verification methods do exist, however.

22. Above all, I want to stress that informing and raising the awareness of children, parents, legal guardians and educational staff about good cybersecurity practices are of the utmost importance. Second, it is clear that website providers must be held responsible for the content they host. Such responsibility and liability can usually already be found in national and European law including the obligation of websites to conduct age verification when providing specific contents or goods. There is a correlation between the requirement for age verification offline and online and such requirement must be applied and enforced effectively in both worlds. It is necessary to reinforce legal requirements for such age verification processes online, given that the digital world provides access to dangerous and risky content from anywhere in the world, without the child leaving their supposedly safe place, at home.

23. There are several options on how to achieve a proper age verification process, for instance through a payment card validation, an offline verification system by buying a "scratch card" in a shop or supermarket to retrieve a login identifier and password, an analysis of identity documentation, or the use of tools provided by central government to verify identity and age.[43]

24. When choosing a method, the following three criteria should be applied: sufficiently reliable verification, complete coverage of the population and respect for the protection of the individual's data, privacy and security, especially confidentiality of information and minimising data exchange.

25. Preventing the exposure of children to pornography is particularly important, given the established effects on behaviour and development. A 2015 meta-analysis of 22 studies from seven countries found that pornography consumption was significantly associated with an increase in verbal and physical aggression.[44] There is also a link between pornography consumption and compulsive sexual behaviour disorder.[45] Moreover, a correlation between pornography and sexual violence between young people has been established.[46] Children must be protected from adults but also from other children in this matter. Pornography must be understood as a public health issue, for which States are responsible for taking appropriate measures, including education and awareness-raising measures.[47] The minimum standard to protect children should be age verification obligations on websites, particularly on sites providing goods and content which are not intended for children and which would incur similar obligations in the offline world.

26. In order to ensure a safe online environment, measures should be put in place to allow for easy reporting of harmful content, pornographic or otherwise. Providers must, moreover, proactively moderate the content themselves, for instance through detection tools or specially trained units. In 2022, the ICSE database identified 4 693 websites containing 121 276 links to child pornographic material. The forthcoming updated version of this database will use the latest technology and AI and will therefore be even more effective. To access the database, States need specialised national units. However, in Africa and Asia there is a serious lack of such units and eight member States of the Council of Europe have not yet created specialised units.[48] In order to effectively fight child sexual exploitation online, all Council of Europe member States should join the ICSE database and special national units should be created wherever they do not yet exist.

27. AI can play a crucial role in the fight to protect children online. It provides a fast and automatic means of verifying and reporting content which is potentially harmful, as well as possibilities to identify victims and offenders. However, its use entails risks, too, linked *inter alia* to the right to privacy and right to protection of

---

42. CNIL, "Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy". Génération numérique, Survey on "Digital practices of young people aged 11 to 18", March 2021.
43. CNIL, "Online age verification: balancing privacy and the protection of minors", 22 September 2022.
44. Paul J. Wright, Robert S. Tokunaga, and Ashley Kraus, "A Meta-Analysis of Pornography Consumption and Actual Acts of Sexual Aggression in General Population Studies", *Journal of Communication* 66, No. 1 (February 2016), pp. 183-205.
45. WHO, International Classification of Diseases ICD-11.
46. Bonino S., Ciairano S., Rabaglietti E., Cattelino E., (2006), "Use of pornography and self-reported engagement in sexual violence among adolescents", *European Journal of Developmental Psychology*, No. 3.
47. "Children, Internet & Pornography", European Centre for Law and Justice (ECLJ), "Contribution to the PACE Committee on Social Affairs".
48. Public hearing on the "Right of the child to protection while using the internet" , *op. cit*.

personal data. It is a valuable tool for strengthening the protection of children online, but must be used within a clear and comprehensive legal framework. Here, too, involving the tech companies in the development of such a framework is paramount.

28. The Council of Europe is currently working on a framework convention to regulate artificial intelligence taking a transversal approach.[49] The framework is based on the Council of Europe's standards on human rights, democracy and the rule of law.[50] The work must also address in sufficient detail the right of the child to protection while on the internet. The Steering Committee for the Rights of the Child has identified the three key challenges that remain in this regard, namely the lack of legal frameworks that address children's rights in the context of artificial intelligence combined with the insufficient enforcement of existing legal frameworks; the fact that artificial intelligence systems are designed in a way that does not consider the specific needs of and risks for children; and the need for better scientific evidence about the impact of artificial intelligence on children's development.[51] The legal framework that the Council of Europe is currently working on presents the perfect opportunity to fill these gaps in the protection of children and I urge those engaged in this work to keep this aspect at the forefront.

29. Regarding communication surveillance, for instance the "flagging" and reporting of harmful content, it must be ensured that children's rights are not harmed. Governments and private companies may collect data from children in the reporting process, and the availability of such data can have harmful consequences for children when they become adults.[52] Therefore, communication surveillance should only be used to serve the child's right to protection while using the internet, and for the timely detection and removal of harmful content within the limits of the law.

4. The legal framework

4.1. United Nations

30. The legal framework on the protection of children on the internet is permanently under construction and is necessarily rapidly changing and adapting to new challenges. At the centre of this framework remains, however, the United Nations Convention on the Rights of the Child (UNCRC) and its protocols.[53] The Council of Europe Strategy for the Rights of the Child (2022-2027) reaffirms that "the UNCRC will remain a key reference for any action deployed by the Council of Europe in this area". Specific attention should always be paid to the four general principles laid down in Article 2 (non-discrimination), Article 3 (best interest of the child), Article 6 (right to life, survival and development) and Article 12 (right to be heard) of the UNCRC.

31. General Comment No. 25 of the United Nations Committee on the Rights of the Child provides an evidence-based and principled guidance for States and other relevant stakeholders for the interpretation of the UNCRC in the digital age. General Comment No. 25 not only raises awareness of the risks children face online, but also places responsibility on countries and businesses to take action to address those risks. It targets key stakeholders to ensure that they acknowledge the importance of children's rights in digital environments. It reaffirms the founding principles of children's rights, including their right to protection from abuse, exploitation and other forms of violence on the internet. It calls for greater action and institutional capacity in situations of violence and abuse against children, and for greater responsibility for States and the private sector to provide a safe-by-design digital environment for children. It also pushes for international harmonisation on this issue, as threats to children's safety online cross borders.

32. More precisely, the General Comment points out that measures need to be child-friendly and age-appropriate. It sets out States' duty to render appropriate assistance to parents and caregivers in the performance of their child-rearing responsibilities. Programmes that create awareness of the risks and provide parents with digital literacy are needed so that they can assist children directly to realise their own rights online, including protection.[54] Moreover, governmental websites informing parents about possible risks and raising awareness of steps that can be taken should be standard.

---

49. "The Council of Europe and artificial intelligence", (website).
50. Decision of the Committee of Ministers, Hamburg, 21 May 2021.
51. "The Council of Europe and artificial intelligence", *op. cit*.
52. UNICEF, "State surveillance and implications for children".
53. Especially the Optional Protocol on the sale of children, child prostitution and child pornography (2000) and the Optional Protocol on a communications procedure (2011). This Convention applies offline and online (see General Comment No. 25 (2021) on children's rights in relation to the digital environment adopted in February 2021 by the UN Committee on the Rights of the Child).
54. General Comment No. 25 (2021).

33. I want to stress that violations of children's rights in a digital environment need to be addressed specifically in national legislation. National legislation that reflects international human rights standards and the rights of children online is imperative and must work alongside a comprehensive, continually updated policy and strategy on how to achieve these rights. It is recommended that States identify a responsible government body for this task which should engage with schools and the technology sector.[55]

34. Access to justice for children who have suffered harm still poses a huge challenge. This is mostly due to a lack of legislation directly prohibiting violations of children's rights in the context of the digital environment.[56] Member States should implement specific legislation. Furthermore, States should offer special training regarding child rights violations online to law enforcement authorities and judges to equip them with the necessary tools and knowledge. The re-traumatisation of the child in the prosecution process is a particular challenge which law enforcement authorities and judges need to bear in mind and prevent.

4.2. Council of Europe

35. The European Convention on Human Rights and its Protocols also contribute to the protection of the rights of the child, be it online or offline. Article 8 of the Convention has been broadened to include online data protection. Article 10 applies to online forms of expression and means of receiving or accessing information. The right to freedom of assembly and association enshrined in Article 11 applies online as well. The specific issue of poor internet connection hindering access to online education (Article 2 of the Additional Protocol to the Convention (ETS No. 9, right to education) has also been raised. As rapporteur, I am not willing to include the latter issue in the scope of my report, as it is not directly linked to the protection of children while using the internet.

36. The case law of the European Court of Human Rights is also relevant here. In the case of *K.U. v.Finland*,[57] the Court found a violation of Article 8 of the Convention on account of the lack of a legal basis enabling the authorities to oblige an internet access provider to disclose the identity of a person wanted for placing an indecent advertisement concerning a minor on a dating site. The legislation must provide the framework for reconciling the various claims which compete for protection in this context.

37. The Council of Europe has developed other treaty instruments applying to the protection of children on the internet. Indeed, all rights of the child that apply offline should apply online. The rights covered by the following are therefore particularly relevant: the European Social Charter (revised) (ETS No. 163), the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, the "Lanzarote Convention"), the Convention on Action against Trafficking in Human Beings (CETS No. 197) and the Convention on preventing and combating violence against women and domestic violence (CETS No. 210, the "Istanbul Convention"). Moreover, specific problems linked to the online world are targeted by other Council of Europe conventions, for instance the Convention on Cybercrime (ETS No. 185, the "Budapest Convention") and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), or the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

38. The Lanzarote Convention is of special importance regarding the right to protection of the child from sexual violence while using the internet. It is also open to accession for non-member States of the Council of Europe, which broadens its application and impact on the protection of children.[58] The convention has so far been ratified by all Council of Europe member States, the Russian Federation and Tunisia.[59] In order to ensure the widest possible protection of children worldwide, I believe that other States should accede to this convention, first and foremost the observer States and States whose parliaments enjoy observer or partner for Democracy status with the Assembly. Similarly, I believe it is important to encourage the signing of, or accession to, the Budapest Convention,[60] which provides for the criminalisation of all offences related to child pornography.

39. The Lanzarote Convention sets out to provide a framework for child-friendly, multidisciplinary and interagency (MDIA) collaboration including co-ordination (Article 10) interviews with the child (Article 35) and protection measures and assistance to victims (Articles 11, 14 and 31). It is internationally recognised that MDIA services are important for child victims and witnesses of violence.[61] The EU Directives on Victims'

55. *Idem*.
56. *Idem*.
57. K.U. v. Finland, No. 2872/02, para. 49, 50, 2 December 2008.
58. See Article 46 of the Lanzarote Convention.
59. Chart of signatures and ratifications of the Lanzarote Convention.
60. Chart of signatures and ratifications of the Budapest Convention.

Rights (Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA) and Child Sexual Abuse (see paragraph 48 of the 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) promote the same standards for EU member States.

40. The Joint European Union/Council of Europe *Barnahus* project reflects this idea of creating a safe environment for children by bringing all relevant services together to provide a co-ordinated and effective response for the child and to prevent re-traumatisation during the investigation and judicial proceedings.[62] I think it could be useful to examine how to provide such a response for child victims of online abuse.

41. The Lanzarote Committee monitors the implementation of the Convention by the State Parties. The second monitoring round on the implementation of the Lanzarote Convention focused on the protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs), with particular emphasis on the challenges raised by child self-generated sexual images and/or videos. The implementation report adopted on 10 March 2022 made several recommendations. In particular, it focuses on clarifying legislation for comprehensive coverage of child abuse. The Lanzarote Committee *inter alia* encourages States Parties to introduce explicit references to conduct involving child self-generated sexual images and/or videos in their legal frameworks or to consider criminalising the offence of "grooming", even when it does not lead to either a face-to-face meeting or to producing child sexual abuse material.[63] Croatia, Cyprus, Germany, and Sweden explicitly mention child self-generated sexual material in their national legal frameworks.

42. There are examples of promising practices regarding campaigns to raise awareness of sexual violence and the risks children may face online, such as the Albanian #Openyoureyes campaign, which used a combination of visual message channels to increase the impact of awareness raising, or the SeguraNet project in Portugal, which among other measures created an annual competition for students, parents and teachers on digital safety issues, including sexting and online predators.[64]

43. All State Parties have reporting mechanisms for child abuse in place. However, States must ensure that all existing mechanisms make it easier for child victims to access help and get support. For example, the Irish national centre for combating illegal content has expanded its "Hotline.ie" offer by adding a new reporting service to help young people whose intimate images and videos have been shared online without their consent.[65]

44. Furthermore, two prevention campaigns led by the Internet Watch Foundation in the United Kingdom are an example of good practice. The "Gurls out loud" campaign helps girls aged 11 to 13 years to recognise the actions of offenders and helps them feel empowered to block and report those actions and inform a trusted person[66] "T.A.L.K." is another campaign to raise parental awareness of the risks and to educate the parents to protect their children online.[67]

45. Another important factor in protecting the rights of the child online is co-operation. Article 38 of the Lanzarote Convention lays down the general principles of and measures for international co-operation. Any State Party can ask for assistance to set up activities regarding the implementation of the Council of Europe standards. For example, the initiative WeProtect Global Alliance which aims to end child sexual exploitation and abuse online is the result of 40 European States working together.[68] Other countries should undertake similar action. Co-operation is key to protect the rights of the child while on the internet. I welcome the fact that

---

61. Council of Europe, "Protection of children against sexual exploitation and abuse – Child-friendly, multidisciplinary and interagency response inspired by the Barnahus model".
62. *Idem.*
63. Lanzarote Committee, 10 March 2022, Implementation report, "The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs): Addressing the challenges raised by child self-generated sexual images and/or videos".
64. Factsheet, Lanzarote Committee, key monitoring findings on: "The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs): addressing the challenges raised by child self-generated sexual images and/or videos (CSGIV)".
65. Lanzarote Committee, Implementation report, op. cit.
66. https://gurlsoutloud.com/.
67. https://talk.iwf.org.uk/.
68. WeProtect Global Alliance.

in November 2023, the Council of Europe joined the WeProtect Global Alliance, a coalition of governments, civil society organisations, companies and international organisations committed to combating child sexual exploitation and abuse.[69]

46. At the Council of Europe level, the guidelines and strategies adopted by the Committee of Ministers play a central role in updating the main Council of Europe legal instruments to take into account new developments and challenges on the internet. Specific attention should be paid to the Council of Europe Strategy for the Rights of the Child (2022-2027), which has dedicated its Strategic Objective 3 to ensuring "access to and safe use of technologies for all children", and to the 2018 Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Among other things, Strategic Objective 3 calls for awareness-raising of abusive and sexist use of social media and online threats for children, ensuring the prompt, efficient and appropriate reporting, investigation and prosecution of cases of online child abuse, supporting parents, families, teachers, volunteers and children to prevent such incidents, and educating and helping them.

47. Furthermore, as regards innovation, Strategic Objective 3 advocates inviting business and industry to fulfil their responsibilities towards children, including by undertaking child impact assessments and involving children in the design of digital services and products. The risks posed by artificial intelligence technologies and the benefits arising from them should be analysed, too.[70]

4.3. European Union

48. It should also be noted that the European Union is currently working on updating its legal framework for the protection of children on the internet. At present, the European Union's main instrument in this regard is Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, of which Article 25(1) deals with online child pornography. Data processing is governed by 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.

49. The European Commission adopted a new European strategy for a better internet for kids (BIK+) in May 2022.[71] Recent developments in the relevant legal framework provided by the European Union include a provisional agreement on temporary rules to detect and remove online child abuse, which applies for three years after its publication in the Official Journal.[72] it provides for a derogation from the confidentiality of communications in order to detect cyber grooming. The temporary agreement provided the basis for the latest proposal for a regulation to prevent and combat child sexual abuse and for the Digital Services Act. On 7 February 2024, the European Parliament approved the opening of negotiations with the Council of the European Union to extend this derogation from data protection rules.

50. In March 2023, the European Union confirmed that it will adopt a new legislation to tackle child sexual abuse online. The framework set out by the European Union can be seen as an example of how to further improve national legislation. The main mechanism will be based on a mandatory detection, reporting and removal system. Its main goal is not only to protect children, but also to support victims and to save lives.

51. It will be mandatory for tech companies to follow strict legal procedures if the risk of sexual child abuse on their website is sufficiently high. The first step is a risk assessment, which the tech company must submit to the co-ordinating authority. If this assessment shows a sufficiently high risk, the co-ordinating authority drafts a request for a detection order. This entails the obligation for the company to introduce detection measures, while the user's privacy must always be respected to the greatest extent possible.

52. Second, the tech company concerned must conduct a data protection impact assessment reviewed by the national data protection authority and a competent authority. Lastly, a judicial authority will decide on the request for a detection order, balancing the need for the order and the effectiveness of the safeguards to limit the invasiveness of the measures. Upon detection of abusive material, the reports on it will be checked by a new EU centre and if confirmed, reported to the police.

69. See news item on the Council of Europe website.
70. Council of Europe Strategy for the Rights of the Child (2022-2027).
71. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2825.
72. The final text was published in the Official Journal of the European Union on 30 July 2021.

53. Taking down abusive content is normally a lengthy process and, until now, the decision was left to tech companies, but with the new law, the content which has to be deleted within 24 hours of a judicial removal order is predetermined.[73] This is a huge step in the right direction. Legal clarity is crucial to efficiently combat violations of children's rights online. This topic cannot be left to the tech companies but should be regulated by law.

54. The European Union's Digital Markets Act (which entered into force on 1 November 2022) and Digital Services Act (which came fully into effect on 17 February 2024) are intended to apply. The latter provides for a "flagging" mechanism to report inappropriate content and puts in place mitigation measures such as age verification.

5. Conclusions

55. I strongly believe that the goal we want to achieve is common to all member States: the effective protection of children online. As I have set out, all stakeholders, including but not limited to States, the technology sector, parents and children, need to work together and be involved in the development of measures and policies to attain this goal. Only through such a holistic approach can the safest and most respectful environment be created.

56. Full safety cannot be achieved overnight, and the situation will continue to evolve as technology develops. Our aim must be to shift from a continuum of violence online to one of protection, ensuring that the best interests of the child are safeguarded at all times. It is important to keep in mind that new challenges to the right of the child to protection while using the internet will continue to arise as new technology develops. Current and future obligations and measures must thus be continually reviewed and if necessary adjusted.

57. The starting point for this process is reviewing national legislation and bringing it up to date where needed, in line with all aspects of human rights standards relating in particular to the rights of the child. This process will cover legally binding obligations in the technology sector for the protection of children on websites, including proper age verification as a minimum standard. Alongside legislative measures, States should focus on awareness-raising and information campaigns aimed at developing digital literacy and the empowerment of children online in general. Such campaigns must reach all relevant groups such as parents, caregivers, teachers, law enforcement personnel and, of course, children. The goal should also be to provide for child-friendly support systems. In all measures taken, the most advanced technology, including artificial intelligence, can be seen as an ally in achieving the best results for prevention, detection and removal of harmful content.

58. Children's use of online resources will undoubtedly continue to increase exponentially, and from even earlier ages, and the technology at their fingertips will develop, too. The Council of Europe should play a leading role in ensuring that member States are ready to prevent harm to children through these developments, bringing to bear both its expertise in the rights of the child and human rights in general and also its current work on legal frameworks relating to technology.

59. I therefore suggest that the Assembly should ask Council of Europe member States to:

- take the necessary steps to review and update their national legislation as regards human rights standards to further improve the protection of children online;

- collaborate not only with the other member States regarding the protection of the child while online, but also with all relevant stakeholders, especially the technology sector, and to create child-friendly support systems;

- take into account new forms of online violence, including harmful deepfakes.

60. The Assembly should also recommend that the Committee of Ministers include the issue of online violence against children in its work and that the relevant bodies, including the Lanzarote Committee, focus on preventing abuse and protecting children in the online world, including from new forms of violence. To this end, the Committee of Ministers should also strengthen its co-operation with the technology industry.

73. European Union, How the new EU law to tackle child sexual abuse will make a difference.