United Nations CRC/C/GC/25

Convention on the Rights of the Child

Distr.: General
2 March 2021

Original: English

Committee on the Rights of the Child

General comment No. 25 (2021) on children's rights in relation to the digital environment

I. Introduction

1. The children consulted for the present general comment reported that digital technologies were vital to their current lives and to their future: "By the means of digital technology, we can get information from all around the world"; "[Digital technology] introduced me to major aspects of how I identify myself"; "When you are sad, the Internet can help you [to] see something that brings you joy".[1]

2. The digital environment is constantly evolving and expanding, encompassing information and communications technologies, including digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology.[2]

3. The digital environment is becoming increasingly important across most aspects of children's lives, including during times of crisis, as societal functions, including education, government services and commerce, progressively come to rely upon digital technologies. It affords new opportunities for the realization of children's rights, but also poses the risks of their violation or abuse. During consultations, children expressed the view that the digital environment should support, promote and protect their safe and equitable engagement: "We would like the government, technology companies and teachers to help us [to] manage untrustworthy information online."; "I would like to obtain clarity about what really happens with my data … Why collect it? How is it being collected?"; "I am … worried about my data being shared".[3]

4. The rights of every child must be respected, protected and fulfilled in the digital environment. Innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the Internet. Meaningful access to digital technologies can support children to realize the full range of their civil, political, cultural, economic and social rights. However, if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise.

5. The present general comment draws on the Committee's experience in reviewing States parties' reports, its day of general discussion on digital media and children's rights, the jurisprudence of the human rights treaty bodies, the recommendations of the Human

[1] "Our rights in a digital world", summary report on the consultation of children for the present general comment, pp. 14 and 22. Available from https://5rightsfoundation.com/uploads/Our%20Rights%20in%20a%20Digital%20World.pdf. All references to children's views refer to that report.

[2] A terminology glossary is available on the Committee's webpage: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCRC%2fINF%2f9314&Lang=en.

[3] "Our rights in a digital world", pp. 14, 16, 22 and 25.

Rights Council and the special procedures of the Council, two rounds of consultations with States, experts and other stakeholders on the concept note and advanced draft and an international consultation with 709 children living in a wide variety of circumstances in 28 countries in several regions.

6. The present general comment should be read in conjunction with other relevant general comments of the Committee and its guidelines regarding the implementation of the Optional Protocol to the Convention on the sale of children, child prostitution and child pornography.

II. Objective

7. In the present general comment, the Committee explains how States parties should implement the Convention in relation to the digital environment and provides guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and the Optional Protocols thereto in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment.

III. General principles

8. The following four principles provide a lens through which the implementation of all other rights under the Convention should be viewed. They should serve as a guide for determining the measures needed to guarantee the realization of children's rights in relation to the digital environment.

A. Non-discrimination

9. The right to non-discrimination requires that States parties ensure that all children have equal and effective access to the digital environment in ways that are meaningful for them.[4] States parties should take all measures necessary to overcome digital exclusion. That includes providing free and safe access for children in dedicated public locations and investing in policies and programmes that support all children's affordable access to, and knowledgeable use of, digital technologies in educational settings, communities and homes.

10. Children may be discriminated against by their being excluded from using digital technologies and services or by receiving hateful communications or unfair treatment through use of those technologies. Other forms of discrimination can arise when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child.

11. The Committee calls upon States parties to take proactive measures to prevent discrimination on the basis of sex, disability, socioeconomic background, ethnic or national origin, language or any other grounds, and discrimination against minority and indigenous children, asylum-seeking, refugee and migrant children, lesbian, gay, bisexual, transgender and intersex children, children who are victims and survivors of trafficking or sexual exploitation, children in alternative care, children deprived of liberty and children in other vulnerable situations. Specific measures will be required to close the gender-related digital divide for girls and to ensure that particular attention is given to access, digital literacy, privacy and online safety.

B. Best interests of the child

12. The best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context.[5] The digital environment was not originally designed for

[4] General comment No. 9 (2006), paras. 37–38.

[5] General comment No. 14 (2013), para. 1.

children, yet it plays a significant role in children's lives. States parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration.

13. States parties should involve the national and local bodies that oversee the fulfilment of the rights of children in such actions. In considering the best interests of the child, they should have regard for all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, and ensure transparency in the assessment of the best interests of the child and the criteria that have been applied.

C. Right to life, survival and development

14. Opportunities provided by the digital environment play an increasingly crucial role in children's development and may be vital for children's life and survival, especially in situations of crisis. States parties should take all appropriate measures to protect children from risks to their right to life, survival and development. Risks relating to content, contact, conduct and contract encompass, among other things, violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist. States parties should identify and address the emerging risks that children face in diverse contexts, including by listening to their views on the nature of the particular risks that they face.

15. The use of digital devices should not be harmful, nor should it be a substitute for in-person interactions among children or between children and parents or caregivers. States parties should pay specific attention to the effects of technology in the earliest years of life, when brain plasticity is maximal and the social environment, in particular relationships with parents and caregivers, is crucial to shaping children's cognitive, emotional and social development. In the early years, precautions may be required, depending on the design, purpose and uses of technologies. Training and advice on the appropriate use of digital devices should be given to parents, caregivers, educators and other relevant actors, taking into account the research on the effects of digital technologies on children's development, especially during the critical neurological growth spurts of early childhood and adolescence.[6]

D. Respect for the views of the child

16. Children reported that the digital environment afforded them crucial opportunities for their voices to be heard in matters that affected them.[7] The use of digital technologies can help to realize children's participation at the local, national and international levels.[8] States parties should promote awareness of, and access to, digital means for children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed, so that they can be effective advocates for their rights, individually and as a group.

17. When developing legislation, policies, programmes, services and training on children's rights in relation to the digital environment, States parties should involve all children, listen to their needs and give due weight to their views. They should ensure that digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services.

18. States parties are encouraged to utilize the digital environment to consult with children on relevant legislative, administrative and other measures and to ensure that their views are considered seriously and that children's participation does not result in undue monitoring or data collection that violates their right to privacy, freedom of thought and opinion. They

[6] General comment No. 24 (2019), para. 22; and general comment No. 20 (2016), paras. 9–11.
[7] "Our rights in a digital world", p. 17.
[8] General comment No. 14 (2013), paras. 89–91.

should ensure that consultative processes are inclusive of children who lack access to technology or the skills to use it.

IV. Evolving capacities

19. States parties should respect the evolving capacities of the child as an enabling principle that addresses the process of their gradual acquisition of competencies, understanding and agency. [9] That process has particular significance in the digital environment, where children can engage more independently from supervision by parents and caregivers. The risks and opportunities associated with children's engagement in the digital environment change depending on their age and stage of development. They should be guided by those considerations whenever they are designing measures to protect children in, or facilitate their access to, that environment. The design of age-appropriate measures should be informed by the best and most up-to-date research available, from a range of disciplines.

20. States parties should take into account the changing position of children and their agency in the modern world, children's competence and understanding, which develop unevenly across areas of skill and activity, and the diverse nature of the risks involved. Those considerations must be balanced with the importance of exercising their rights in supported environments and the range of individual experiences and circumstances.[10] States parties should ensure that digital service providers offer services that are appropriate for children's evolving capacities.

21. In accordance with States' duty to render appropriate assistance to parents and caregivers in the performance of their child-rearing responsibilities, States parties should promote awareness among parents and caregivers of the need to respect children's evolving autonomy, capacities and privacy. They should support parents and caregivers in acquiring digital literacy and awareness of the risks to children in order to help them to assist children in the realization of their rights, including to protection, in relation to the digital environment.

V. General measures of implementation by States parties

22. Opportunities for the realization of children's rights and their protection in the digital environment require a broad range of legislative, administrative and other measures, including precautionary ones.

A. Legislation

23. States parties should review, adopt and update national legislation in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention and the Optional Protocols thereto. Legislation should remain relevant, in the context of technological advances and emerging practices. They should mandate the use of child rights impact assessments to embed children's rights into legislation, budgetary allocations and other administrative decisions relating to the digital environment and promote their use among public bodies and businesses relating to the digital environment.[11]

B. Comprehensive policy and strategy

24. States parties should ensure that national policies relating to children's rights specifically address the digital environment, and they should implement regulation, industry

[9] General comment No. 7 (2005), para. 17; and general comment No. 20 (2016), paras. 18 and 20.
[10] General comment No. 20 (2016), para. 20.
[11] General comment No. 5 (2003), para. 45; general comment No. 14 (2013), para. 99; and general comment No. 16 (2013), paras. 78–81.

codes, design standards and action plans accordingly, all of which should be regularly evaluated and updated. Such national policies should be aimed at providing children with the opportunity to benefit from engaging with the digital environment and ensuring their safe access to it.

25. Children's online protection should be integrated within national child protection policies. States parties should implement measures that protect children from risks, including cyberaggression and digital technology-facilitated and online child sexual exploitation and abuse, ensure the investigation of such crimes and provide remedy and support for children who are victims. They should also address the needs of children in disadvantaged or vulnerable situations, including by providing child-friendly information that is, when necessary, translated into relevant minority languages.

26. States parties should ensure the operation of effective child protection mechanisms online and safeguarding policies, while also respecting children's other rights, in all settings where children access the digital environment, which includes the home, educational settings, cybercafés, youth centres, libraries and health and alternative care settings.

C. Coordination

27. To encompass the cross-cutting consequences of the digital environment for children's rights, States parties should identify a government body that is mandated to coordinate policies, guidelines and programmes relating to children's rights among central government departments and the various levels of government.[12] Such a national coordination mechanism should engage with schools and the information and communications technology sector and cooperate with businesses, civil society, academia and organizations to realize children's rights in relation to the digital environment at the cross-sectoral, national, regional and local levels.[13] It should draw on technological and other relevant expertise within and beyond government, as needed, and be independently evaluated for its effectiveness in meeting its obligations.

D. Allocation of resources

28. States parties should mobilize, allocate and utilize public resources to implement legislation, policies and programmes to fully realize children's rights in the digital environment and to improve digital inclusion, which is needed to address the increasing impact of the digital environment on children's lives and to promote the equality of access to, and affordability of, services and connectivity.[14]

29. Where resources are contributed from the business sector or obtained through international cooperation, States parties should ensure that their own mandate, revenue mobilization, budget allocations and expenditure are not interfered with or undermined by third parties.[15]

E. Data collection and research

30. Regularly updated data and research are crucial to understanding the implications of the digital environment for children's lives, evaluating its impact on their rights and assessing the effectiveness of State interventions. States parties should ensure the collection of robust, comprehensive data that is adequately resourced and that data are disaggregated by age, sex, disability, geographical location, ethnic and national origin and socioeconomic background. Such data and research, including research conducted with and by children, should inform legislation, policy and practice and should be available in the public domain.[16] Data

[12] General comment No. 5 (2003), para. 37.
[13] Ibid., paras. 27 and 39.
[14] General comment No. 19 (2016), para. 21.
[15] Ibid., para. 27 (b).
[16] General comment No. 5 (2003), paras. 48 and 50.

collection and research relating to children's digital lives must respect their privacy and meet the highest ethical standards.

F. Independent monitoring

31. States parties should ensure that the mandates of national human rights institutions and other appropriate independent institutions cover children's rights in the digital environment and that they are able to receive, investigate and address complaints from children and their representatives.[17] Where independent oversight bodies exist to monitor activities in relation to the digital environment, national human rights institutions should work closely with such bodies on effectively discharging their mandate regarding children's rights.[18]

G. Dissemination of information, awareness-raising and training

32. States parties should disseminate information and conduct awareness-raising campaigns on the rights of the child in the digital environment, focusing in particular on those whose actions have a direct or indirect impact on children. They should facilitate educational programmes for children, parents and caregivers, the general public and policymakers to enhance their knowledge of children's rights in relation to the opportunities and risks associated with digital products and services. Such programmes should include information on how children can benefit from digital products and services and develop their digital literacy and skills, how to protect children's privacy and prevent victimization and how to recognize a child who is a victim of harm perpetrated online or offline and respond appropriately. Such programmes should be informed by research and consultations with children, parents and caregivers.

33. Professionals working for and with children and the business sector, including the technology industry, should receive training that includes how the digital environment affects the rights of the child in multiple contexts, the ways in which children exercise their rights in the digital environment and how they access and use technologies. They should also receive training on the application of international human rights standards to the digital environment. States parties should ensure that pre-service and in-service training relating to the digital environment is provided for professionals working at all levels of education, to support the development of their knowledge, skills and practice.

H. Cooperation with civil society

34. States parties should systematically involve civil society, including child-led groups and non-governmental organizations working in the field of children's rights and those concerned with the digital environment, in the development, implementation, monitoring and evaluation of laws, policies, plans and programmes relating to children's rights. They should also ensure that civil society organizations are able to implement their activities relating to the promotion and protection of children's rights in relation to the digital environment.

I. Children's rights and the business sector

35. The business sector, including not-for-profit organizations, affects children's rights directly and indirectly in the provision of services and products relating to the digital environment. Businesses should respect children's rights and prevent and remedy abuse of their rights in relation to the digital environment. States parties have the obligation to ensure that businesses meet those responsibilities.[19]

[17] General comment No. 2 (2002), paras. 2 and 7.
[18] Ibid., para. 7.
[19] General comment No. 16 (2013), paras. 28, 42 and 82.

36. States parties should take measures, including through the development, monitoring, implementation and evaluation of legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies. They should also encourage businesses to provide public information and accessible and timely advice to support children's safe and beneficial digital activities.

37. States parties have a duty to protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment. Although businesses may not be directly involved in perpetrating harmful acts, they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services. States parties should put in place, monitor and enforce laws and regulations aimed at preventing violations of the right to protection from violence, as well as those aimed at investigating, adjudicating on and redressing violations as they occur in relation to the digital environment.[20]

38. States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children.[21] They should take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses.

39. In addition to developing legislation and policies, States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child. They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service.

J. Commercial advertising and marketing

40. The digital environment includes businesses that rely financially on processing personal data to target revenue-generating or paid-for content, and such processes intentionally and unintentionally affect the digital experiences of children. Many of those processes involve multiple commercial partners, creating a supply chain of commercial activity and the processing of personal data that may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content.

41. States parties should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes.

42. States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products,

[20] Ibid., para. 60.

[21] Ibid., paras. 50 and 62–65.

applications and services should also be prohibited from engagement directly or indirectly with children.

K. Access to justice and remedies

43. Children face particular challenges in access to justice relating to the digital environment for a range of reasons. Such challenges arise because of the lack of legislation placing sanctions on children's rights violations specifically in relation to the digital environment, the difficulties in obtaining evidence or identifying perpetrators or because children and their parents or caregivers lack knowledge of their rights or of what constitutes a violation or abuse of their rights in the digital environment, among other factors. Further challenges may arise if children are required to disclose sensitive or private online activities or from their fear of reprisals by peers or of social exclusion.

44. States parties should ensure that appropriate and effective remedial judicial and non-judicial mechanisms for the violations of children's rights relating to the digital environment are widely known and readily available to all children and their representatives. Complaint and reporting mechanisms should be free of charge, safe, confidential, responsive, child-friendly and available in accessible formats. States parties should also provide for collective complaints, including class action and public interest litigation, and for legal or other appropriate assistance, including through specialized services, to children whose rights have been violated in or through the digital environment.

45. States parties should establish, coordinate and regularly monitor and evaluate frameworks for the referral of such cases and the provision of effective support to children who are victims.[22] Frameworks should include measures for the identification of, therapy and follow-up care for, and the social reintegration of, children who are victims. Training on the identification of children who are victims should be included in referral mechanisms, including for digital service providers. Measures within such a framework should be multi-agency and child-friendly, to prevent a child's revictimization and secondary victimization in the context of investigative and judicial processes. That may require specialized protections for confidentiality and to redress harms associated with the digital environment.

46. Appropriate reparation includes restitution, compensation and satisfaction and may require apology, correction, removal of unlawful content, access to psychological recovery services or other measures.[23] In relation to violations in the digital environment, remedial mechanisms should take into account the vulnerability of children and the need to be swift to halt ongoing and future damage. States parties should guarantee the non-recurrence of violations, including by the reform of relevant laws and policies and their effective implementation.

47. Digital technologies bring additional complexity to the investigation and prosecution of crimes against children, which may cross national borders. States parties should address the ways in which uses of digital technologies may facilitate or impede the investigation and prosecution of crimes against children and take all available preventative, enforcement and remedial measures, including in cooperation with international partners. They should provide specialized training for law enforcement officials, prosecutors and judges regarding child rights violations specifically associated with the digital environment, including through international cooperation.

48. Children may face particular difficulties in obtaining remedy when their rights have been abused in the digital environment by business enterprises, in particular in the context of their global operations.[24] States parties should consider measures to respect, protect and fulfil children's rights in the context of businesses' extraterritorial activities and operations, provided that there is a reasonable link between the State and the conduct concerned. They should ensure that businesses provide effective complaint mechanisms; such mechanisms should not, however, prevent children from gaining access to State-based remedies. They

[22] General comment No. 21 (2017), para. 22. See also General Assembly resolution 60/147, annex.
[23] General comment No. 5 (2003), para. 24.
[24] General comment No. 16 (2013), paras. 66–67.

should also ensure that agencies with oversight powers relevant to children's rights, such as those relating to health and safety, data protection and consumer rights, education and advertising and marketing, investigate complaints and provide adequate remedies for violations or abuses of children's rights in the digital environment.[25]

49. States parties should provide children with child-sensitive and age-appropriate information in child-friendly language on their rights and on the reporting and complaint mechanisms, services and remedies available to them in cases where their rights in relation to the digital environment are violated or abused. Such information should also be provided to parents, caregivers and professionals working with and for children.

VI. Civil rights and freedoms

A. Access to information

50. The digital environment provides a unique opportunity for children to realize the right to access to information. In that regard, information and communications media, including digital and online content, perform an important function.[26] States parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary for the purposes stipulated in article 13 of the Convention.

51. States parties should provide and support the creation of age-appropriate and empowering digital content for children in accordance with children's evolving capacities and ensure that children have access to a wide diversity of information, including information held by public bodies, about culture, sports, the arts, health, civil and political affairs and children's rights.

52. States parties should encourage the production and dissemination of such content using multiple formats and from a plurality of national and international sources, including news media, broadcasters, museums, libraries and educational, scientific and cultural organizations. They should particularly endeavour to enhance the provision of diverse, accessible and beneficial content for children with disabilities and children belonging to ethnic, linguistic, indigenous and other minority groups. The ability to access relevant information, in the languages that children understand, can have a significant positive impact on equality.[27]

53. States parties should ensure that all children are informed about, and can easily find, diverse and good quality information online, including content independent of commercial or political interests. They should ensure that automated search and information filtering, including recommendation systems, do not prioritize paid content with a commercial or political motivation over children's choices or at the cost of children's right to information.

54. The digital environment can include gender-stereotyped, discriminatory, racist, violent, pornographic and exploitative information, as well as false narratives, misinformation and disinformation and information encouraging children to engage in unlawful or harmful activities. Such information may come from multiple sources, including other users, commercial content creators, sexual offenders or armed groups designated as terrorist or violent extremist. States parties should protect children from harmful and untrustworthy content and ensure that relevant businesses and other providers of digital content develop and implement guidelines to enable children to safely access diverse content, recognizing children's rights to information and freedom of expression, while protecting them from such harmful material in accordance with their rights and evolving capacities.[28] Any restrictions on the operation of any Internet-based, electronic or other information

[25] Ibid., paras. 30 and 43.
[26] General comment No. 7 (2005), para. 35; and general comment No. 20 (2016), para. 47.
[27] General comment No. 17 (2013), para. 46; and general comment No. 20 (2016), paras. 47–48.
[28] General comment No. 16 (2013), para. 58; and general comment No. 7 (2005), para. 35.

dissemination systems should be in line with article 13 of the Convention.[29] States parties should not intentionally obstruct or enable other actors to obstruct the supply of electricity, cellular networks or Internet connectivity in any geographical area, whether in part or as a whole, which can have the effect of hindering a child's access to information and communication.

55. States parties should encourage providers of digital services used by children to apply concise and intelligible content labelling, for example on the age-appropriateness or trustworthiness of content. They should also encourage the provision of accessible guidance, training, educational materials and reporting mechanisms for children, parents and caregivers, educators and relevant professional groups.[30] Age-based or content-based systems designed to protect children from age-inappropriate content should be consistent with the principle of data minimization.

56. States parties should ensure that digital service providers comply with relevant guidelines, standards and codes[31] and enforce lawful, necessary and proportionate content moderation rules. Content controls, school filtering systems and other safety-oriented technologies should not be used to restrict children's access to information in the digital environment; they should be used only to prevent the flow of harmful material to children. Content moderation and content controls should be balanced with the right to protection against violations of children's other rights, notably their rights to freedom of expression and privacy.

57. Professional codes of conduct set by news media and other relevant organizations should include guidance on how to report digital risks and opportunities relating to children. Such guidance should result in evidence-based reporting that does not reveal the identity of children who are victims and survivors and that is in accordance with international human rights standards.

B. Freedom of expression

58. Children's right to freedom of expression includes the freedom to seek, receive and impart information and ideas of all kinds, using any media of their choice. Children reported[32] that the digital environment offered significant scope to express their ideas, opinions and political views. For children in disadvantaged or vulnerable situations, technology-facilitated interaction with others who share their experiences can help them to express themselves.

59. Any restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate. The rationale for such restrictions should be transparent and communicated to children in age-appropriate language. States parties should provide children with information and training opportunities on how to effectively exercise that right, in particular how to create and share digital content safely, while respecting the rights and dignity of others and not violating legislation, such as that relating to incitement to hatred and violence.

60. When children express their political or other views and identities in the digital environment, they may attract criticism, hostility, threats or punishment. States parties should protect children from cyberaggression and threats, censorship, data breaches and digital surveillance. Children should not be prosecuted for expressing their opinions in the digital environment, unless they violate restrictions provided by criminal legislation which are compatible with article 13 of the Convention.

61. Given the existence of commercial and political motivations to promote particular world views, States parties should ensure that uses of automated processes of information filtering, profiling, marketing and decision-making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment.

[29] Human Rights Committee, general comment No. 34 (2011), para. 43.
[30] General comment No. 16 (2013), paras. 19 and 59.
[31] Ibid., paras. 58 and 61.
[32] "Our rights in a digital world", p. 16.

C. Freedom of thought, conscience and religion

62. States parties should respect the right of the child to freedom of thought, conscience and religion in the digital environment. The Committee encourages States parties to introduce or update data protection regulation and design standards that identify, define and prohibit practices that manipulate or interfere with children's right to freedom of thought and belief in the digital environment, for example by emotional analytics or inference. Automated systems may be used to make inferences about a child's inner state. They should ensure that automated systems or information filtering systems are not used to affect or influence children's behaviour or emotions or to limit their opportunities or development.

63. States parties should ensure that children are not penalized for their religion or beliefs or have their future opportunities in any other way restricted. The exercise of children's right to manifest their religion or beliefs in the digital environment may be subject only to limitations that are lawful, necessary and proportionate.

D. Freedom of association and peaceful assembly

64. The digital environment can enable children to form their social, religious, cultural, ethnic, sexual and political identities and to participate in associated communities and in public spaces for deliberation, cultural exchange, social cohesion and diversity.[33] Children reported that the digital environment provided them with valued opportunities to meet, exchange and deliberate with peers, decision makers and others who shared their interests.[34]

65. States parties should ensure that their laws, regulations and policies protect children's right to participate in organizations that operate partially or exclusively in the digital environment. No restrictions may be placed on the exercise by children of their right to freedom of association and peaceful assembly in the digital environment other than those that are lawful, necessary and proportionate.[35] Such participation should not in and of itself result in negative consequences to those children, such as exclusion from a school, restriction or deprivation of future opportunities or creation of a police profile. Such participation should be safe, private and free from surveillance by public or private entities.

66. Public visibility and networking opportunities in the digital environment can also support child-led activism and can empower children as advocates for human rights. The Committee recognizes that the digital environment enables children, including children human rights defenders, as well as children in vulnerable situations, to communicate with each other, advocate for their rights and form associations. States parties should support them, including by facilitating the creation of specific digital spaces, and ensure their safety.

E. Right to privacy

67. Privacy is vital to children's agency, dignity and safety and for the exercise of their rights. Children's personal data are processed to offer educational, health and other benefits to them. Threats to children's privacy may arise from data collection and processing by public institutions, businesses and other organizations, as well as from such criminal activities as identity theft. Threats may also arise from children's own activities and from the activities of family members, peers or others, for example, by parents sharing photographs online or a stranger sharing information about a child.

68. Data may include information about, inter alia, children's identities, activities, location, communication, emotions, health and relationships. Certain combinations of personal data, including biometric data, can uniquely identify a child. Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy; they may have

[33] General comment No. 17 (2013), para. 21; and general comment No. 20 (2016), paras. 44–45.

[34] "Our rights in a digital world", p. 20.

[35] Human Rights Committee, general comment No. 37 (2020), paras. 6 and 34.

adverse consequences on children, which can continue to affect them at later stages of their lives.

69. Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention.

70. States parties should take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Legislation should include strong safeguards, transparency, independent oversight and access to remedy. States parties should require the integration of privacy-by-design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. Where encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. Such measures must be strictly limited according to the principles of legality, necessity and proportionality.

71. Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver.

72. States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations.[36] They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats.

73. Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures.[37] Children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child, parent or caregiver, as appropriate.

74. Privacy and data protection legislation and measures should not arbitrarily limit children's other rights, such as their right to freedom of expression or protection. States parties should ensure that data protection legislation respects children's privacy and personal data in relation to the digital environment. Through continual technological innovation, the scope of the digital environment is expanding to include ever more services and products, such as clothes and toys. As settings where children spend time become "connected", through the use of embedded sensors connected to automated systems, States parties should ensure that the products and services that contribute to such environments are subject to robust data protection and other privacy regulations and standards. That includes public settings, such as

[36] Human Rights Committee, general comment No. 16 (1988), para. 10.

[37] Ibid.; and Committee on the Rights of the Child, general comment No. 20 (2016), para. 46.

streets, schools, libraries, sports and entertainment venues and business premises, including shops and cinemas, and the home.

75. Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose.

76. The digital environment presents particular problems for parents and caregivers in respecting children's right to privacy. Technologies that monitor online activities for safety purposes, such as tracking devices and services, if not implemented carefully, may prevent a child from accessing a helpline or searching for sensitive information. States parties should advise children, parents and caregivers and the public on the importance of the child's right to privacy and on how their own practices may threaten that right. They should also be advised about the practices through which they can respect and protect children's privacy in relation to the digital environment, while keeping them safe. Parents' and caregivers' monitoring of a child's digital activity should be proportionate and in accordance with the child's evolving capacities.

77. Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should require an approach integrating safety-by-design and privacy-by-design to anonymity, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyberaggression, hate speech or sexual exploitation and abuse. Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care. Such cases may require further intervention, as well as family counselling or other services, to safeguard the child's right to privacy.

78. Providers of preventive or counselling services to children in the digital environment should be exempt from any requirement for a child user to obtain parental consent in order to access such services.[38] Such services should be held to high standards of privacy and child protection.

F. Birth registration and right to identity

79. States parties should promote the use of digital identification systems that enable all newborn children to have their birth registered and officially recognized by the national authorities, in order to facilitate access to services, including health, education and welfare. Lack of birth registration facilitates the violation of children's rights under the Convention and the Optional Protocols thereto. States parties should use up-to-date technology, including mobile registration units, to ensure access to birth registration, especially for children in remote areas, refugee and migrant children, children at risk and those in marginalized situations, and include children born prior to the introduction of digital identification systems. For such systems to benefit children, they should conduct awareness-raising campaigns, establish monitoring mechanisms, promote community engagement and ensure effective coordination between different actors, including civil status officers, judges, notaries, health officials and child protection agency personnel. They should also ensure that a robust privacy and data protection framework is in place.

VII. Violence against children

80. The digital environment may open up new ways to perpetrate violence against children, by facilitating situations in which children experience violence and/or may be

[38] General comment No. 20 (2016), para. 60.

influenced to do harm to themselves or others. Crises, such as pandemics, may lead to an increased risk of harm online, given that children spend more time on virtual platforms in those circumstances.

81. Sexual offenders may use digital technologies to solicit children for sexual purposes and to participate in online child sexual abuse, for example, by the live video streaming, production and distribution of child sexual abuse material and through sexual extortion. Forms of digitally facilitated violence and sexual exploitation and abuse may also be perpetrated within a child's circle of trust, by family or friends or, for adolescents, by intimate partners, and may include cyberaggression, including bullying and threats to reputation, the non-consensual creation or sharing of sexualized text or images, such as self-generated content by solicitation and/or coercion, and the promotion of self-harming behaviours, such as cutting, suicidal behaviour or eating disorders. Where children have carried out such actions, States parties should pursue preventive, safeguarding and restorative justice approaches for the children involved whenever possible.[39]

82. States parties should take legislative and administrative measures to protect children from violence in the digital environment, including the regular review, updating and enforcement of robust legislative, regulatory and institutional frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment. Such risks include physical or mental violence, injury or abuse, neglect or maltreatment, exploitation and abuse, including sexual exploitation and abuse, child trafficking, gender-based violence, cyberaggression, cyberattacks and information warfare. States parties should implement safety and protective measures in accordance with children's evolving capacities.

83. The digital environment can open up new ways for non-State groups, including armed groups designated as terrorist or violent extremist, to recruit and exploit children to engage with or participate in violence. States parties should ensure that legislation prohibits the recruitment of children by terrorist or violent extremist groups. Children accused of criminal offences in that context should be treated primarily as victims but, if charged, the child justice system should apply.

VIII. Family environment and alternative care

84. Many parents and caregivers require support to develop the technological understanding, capacity and skills necessary to assist children in relation to the digital environment. States parties should ensure that parents and caregivers have opportunities to gain digital literacy, to learn how technology can support the rights of children and to recognize a child who is a victim of online harm and respond appropriately. Special attention should be paid to the parents and caregivers of children in disadvantaged or vulnerable situations.

85. In supporting and guiding parents and caregivers regarding the digital environment, States parties should promote their awareness to respect children's growing autonomy and need for privacy, in accordance with their evolving capacities. States parties should take into account that children often embrace and experiment with digital opportunities and may encounter risks, including at a younger age than parents and caregivers may anticipate. Some children reported wanting more support and encouragement in their digital activities, especially where they perceived parents' and caregivers' approach to be punitive, overly restrictive or not adjusted to their evolving capacities.[40]

86. States parties should take into account that support and guidance provided to parents and caregivers should be based on an understanding of the specificity and uniqueness of parent-child relations. Such guidance should support parents in sustaining an appropriate balance between the child's protection and emerging autonomy, based on mutual empathy and respect, over prohibition or control. To help parents and caregivers to maintain a balance between parental responsibilities and children's rights, the best interests of the child, applied

[39] General comment No. 24 (2019), para. 101; and CRC/C/156, para. 71.

[40] "Our rights in a digital world", p. 30.

together with consideration of the child's evolving capacities, should be the guiding principles. Guidance to parents and caregivers should encourage children's social, creative and learning activities in the digital environment and emphasize that the use of digital technologies should not replace direct, responsive interactions among children themselves or between children and parents or caregivers.

87. It is important that children separated from their families have access to digital technologies.[41] Evidence has shown that digital technologies are beneficial in maintaining family relationships, for example, in cases of parental separation, when children are placed in alternative care, for the purposes of establishing relations between children and prospective adoptive or foster parents and in reuniting children in humanitarian crisis situations with their families. Therefore, in the context of separated families, States parties should support access to digital services for children and their parents, caregivers or other relevant persons, taking into consideration the safety and best interests of the child.

88. Measures taken to enhance digital inclusion should be balanced with the need to protect children in cases where parents or other family members or caregivers, whether physically present or distant, may place them at risk. States parties should consider that such risks may be enabled through the design and use of digital technologies, for example, by revealing the location of a child to a potential abuser. In recognition of those risks, They should require an approach integrating safety-by-design and privacy-by-design and ensure that parents and caregivers are fully aware of the risks and available strategies to support and protect children.

IX. Children with disabilities

89. The digital environment opens new avenues for children with disabilities to engage in social relationships with their peers, access information and participate in public decision-making processes. States parties should pursue those avenues and take steps to prevent the creation of new barriers and to remove existing barriers faced by children with disabilities in relation to the digital environment.

90. Children with different types of disabilities, including physical, intellectual, psychosocial, auditory and visual disabilities, face different barriers in accessing the digital environment, such as content in non-accessible formats, limited access to affordable assistive technologies at home, school and in the community and the prohibition of the use of digital devices in schools, health facilities and other environments. States parties should ensure that children with disabilities have access to content in accessible formats and remove policies that have a discriminatory impact on such children. They should ensure access to affordable assistive technologies, where needed, in particular for children with disabilities living in poverty, and provide awareness-raising campaigns, training and resources for children with disabilities, their families and staff in educational and other relevant settings so that they have sufficient knowledge and skills to use digital technologies effectively.

91. States parties should promote technological innovations that meet the requirements of children with different types of disabilities and ensure that digital products and services are designed for universal accessibility so that they can be used by all children without exception and without the need for adaptation. Children with disabilities should be involved in the design and delivery of policies, products and services that affect the realization of their rights in the digital environment.

92. Children with disabilities may be more exposed to risks, including cyberaggression and sexual exploitation and abuse, in the digital environment. States parties should identify and address the risks faced by children with disabilities, taking steps to ensure that the digital environment is safe for them, while countering the prejudice faced by children with disabilities that might lead to overprotection or exclusion. Safety information, protective strategies and public information, services and forums relating to the digital environment should be provided in accessible formats.

[41] General comment No. 21 (2017), para. 35.

X. Health and welfare

93. Digital technologies can facilitate access to health services and information and improve diagnostic and treatment services for maternal, newborn, child and adolescent physical and mental health and nutrition. They also offer significant opportunities for reaching children in disadvantaged or vulnerable situations or in remote communities. In situations of public emergency or in health or humanitarian crises, access to health services and information through digital technologies may become the only option.

94. Children reported that they valued searching online for information and support relating to health and well-being, including on physical, mental and sexual and reproductive health, puberty, sexuality and conception.[42] Adolescents especially wanted access to free, confidential, age-appropriate and non-discriminatory mental health and sexual and reproductive health services online.[43] States parties should ensure that children have safe, secure and confidential access to trustworthy health information and services, including psychological counselling services.[44] Those services should limit the processing of children's data to that which is necessary for the performance of the service and should be provided by professionals or those with appropriate training, with regulated oversight mechanisms in place. States parties should ensure that digital health products and services do not create or increase inequities in children's access to in-person health services.

95. States parties should encourage and invest in research and development that is focused on children's specific health needs and that promotes positive health outcomes for children through technological advances. Digital services should be used to supplement or improve the in-person provision of health services to children.[45] States parties should introduce or update regulation that requires providers of health technologies and services to embed children's rights within the functionality, content and distribution thereof.

96. States parties should regulate against known harms and proactively consider emerging research and evidence in the public health sector, to prevent the spread of misinformation and materials and services that may damage children's mental or physical health. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children's development and rights.[46]

97. States parties should encourage the use of digital technologies to promote healthy lifestyles, including physical and social activity.[47] They should regulate targeted or age-inappropriate advertising, marketing and other relevant digital services to prevent children's exposure to the promotion of unhealthy products, including certain food and beverages, alcohol, drugs and tobacco and other nicotine products.[48] Such regulations relating to the digital environment should be compatible and keep pace with regulations in the offline environment.

98. Digital technologies offer multiple opportunities for children to improve their health and well-being, when balanced with their need for rest, exercise and direct interaction with their peers, families and communities. States parties should develop guidance for children, parents, caregivers and educators regarding the importance of a healthy balance of digital and non-digital activities and sufficient rest.

[42] "Our rights in a digital world", p. 37.
[43] General comment No. 20 (2016), para. 59.
[44] Ibid., paras. 47 and 59.
[45] Ibid., paras. 47–48.
[46] General comment No. 15 (2013), para. 84.
[47] General comment No. 17 (2013), para. 13.
[48] General comment No. 15 (2013), para. 77.

XI. Education, leisure and cultural activities

A. Right to education

99. The digital environment can greatly 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. Use of digital technologies can also strengthen engagement between the teacher and student and between learners. Children highlighted the importance of digital technologies in improving their access to education and in supporting their learning and participation in extracurricular activities.[49]

100. States parties should support educational and cultural institutions, such as archives, libraries and museums, in enabling access for children to diverse digital and interactive learning resources, including indigenous resources, and resources in the languages that children understand. Those and other valuable resources can support children's engagement with their own creative, civic and cultural practices and enable them to learn about those of others.[50] States parties should enhance children's opportunities for online and lifelong learning.

101. States parties should invest equitably in technological infrastructure in schools and other learning settings, ensuring the availability and affordability of a sufficient number of computers, high-quality and high-speed broadband and a stable source of electricity, teacher training on the use of digital educational technologies, accessibility and the timely maintenance of school technologies. They should also support the creation and dissemination of diverse digital educational resources of good quality in the languages that children understand and ensure that existing inequalities are not exacerbated, such as those experienced by girls. States parties should ensure that the use of digital technologies does not undermine in-person education and is justified for educational purposes.

102. For children who are not physically present in school or for those who live in remote areas or in disadvantaged or vulnerable situations, digital educational technologies can enable distance or mobile learning.[51] States parties should ensure that there is proper infrastructure in place to enable access for all children to the basic utilities necessary for distance learning, including access to devices, electricity, connectivity, educational materials and professional support. They should also ensure that schools have sufficient resources to provide parents and caregivers with guidance on remote learning at home and that digital education products and services do not create or exacerbate inequities in children's access to in-person education services.

103. States parties should develop evidence-based policies, standards and guidelines for schools and other relevant bodies responsible for procuring and using educational technologies and materials to enhance the provision of valuable educational benefits. Standards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights, such as the use of digital technologies to document a child's activity and share it with parents or caregivers without the child's knowledge or consent.

104. States parties should ensure that digital literacy is taught in schools, as part of basic education curricula, from the preschool level and throughout all school years, and that such pedagogies are assessed on the basis of their results.[52] Curricula should include the knowledge and skills to safely handle a wide range of digital tools and resources, including those relating to content, creation, collaboration, participation, socialization and civic

[49] "Our rights in a digital world", pp. 14, 16 and 30.

[50] General comment No. 17 (2013), para. 10.

[51] Joint general recommendation No. 31 of the Committee on the Elimination of Discrimination against Women/general comment No. 18 of the Committee on the Rights of the Child (2019), para. 64; and Committee on the Rights of the Child, general comment No. 11 (2009), para. 61; and general comment No. 21 (2017), para. 55.

[52] General comment No. 20 (2016), para. 47.

engagement. Curricula should also include critical understanding, guidance on how to find trusted sources of information and to identify misinformation and other forms of biased or false content, including on sexual and reproductive health issues, human rights, including the rights of the child in the digital environment, and available forms of support and remedy. They should promote awareness among children of the possible adverse consequences of exposure to risks relating to content, contact, conduct and contract, including cyberaggression, trafficking, sexual exploitation and abuse and other forms of violence, as well as coping strategies to reduce harm and strategies to protect their personal data and those of others and to build children's social and emotional skills and resilience.

105. It is of increasing importance that children gain an understanding of the digital environment, including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies. Teachers, in particular those who undertake digital literacy education and sexual and reproductive health education, should be trained on safeguards relating to the digital environment.

B. Right to culture, leisure and play

106. The digital environment promotes children's right to culture, leisure and play, which is essential for their well-being and development.[53] Children of all ages reported that they experienced pleasure, interest and relaxation through engaging with a wide range of digital products and services of their choice,[54] but that they were concerned that adults might not understand the importance of digital play and how it could be shared with friends.[55]

107. Digital forms of culture, recreation and play should support and benefit children and reflect and promote children's differing identities, in particular their cultural identities, languages and heritage. They can facilitate children's social skills, learning, expression, creative activities, such as music and art, and sense of belonging and a shared culture.[56] Participation in cultural life online contributes to creativity, identity, social cohesiveness and cultural diversity. States parties should ensure that children have the opportunity to use their free time to experiment with information and communications technologies, express themselves and participate in cultural life online.

108. States parties should regulate and provide guidance for professionals, parents and caregivers and collaborate with digital service providers, as appropriate, to ensure that digital technologies and services intended for, accessed by or having an impact on children in their leisure time are designed, distributed and used in ways that enhance children's opportunities for culture, recreation and play. That can include encouraging innovation in digital play and related activities that support children's autonomy, personal development and enjoyment.

109. States parties should ensure that the promotion of opportunities for culture, leisure and play in the digital environment is balanced with the provision of attractive alternatives in the physical locations where children live. Especially in their early years, children acquire language, coordination, social skills and emotional intelligence largely through play that involves physical movement and direct face-to-face interaction with other people. For older children, play and recreation that involve physical activities, team sports and other outdoor recreational activities can provide health benefits, as well as functional and social skills.

110. Leisure time spent in the digital environment may expose children to risks of harm, for example, through opaque or misleading advertising or highly persuasive or gambling-like design features. By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child.

[53] General comment No. 17 (2013), para. 7.
[54] "Our rights in a digital world", p. 22.
[55] General comment No. 17 (2013), para. 33.
[56] Ibid., para. 5.

111. Where States parties or businesses provide guidance, age ratings, labelling or certification regarding certain forms of digital play and recreation, they should be formulated so as not to curtail children's access to the digital environment as a whole or interfere with their opportunities for leisure or their other rights.

XII. Special protection measures

A. Protection from economic, sexual and other forms of exploitation

112. Children should be protected from all forms of exploitation prejudicial to any aspects of their welfare in relation to the digital environment. Exploitation may occur in many forms, such as economic exploitation, including child labour, sexual exploitation and abuse, the sale, trafficking and abduction of children and the recruitment of children to participate in criminal activities, including forms of cybercrime. By creating and sharing content, children may be economic actors in the digital environment, which may result in their exploitation.

113. States parties should review relevant laws and policies to ensure that children are protected against economic, sexual and other forms of exploitation and that their rights with regard to work in the digital environment and related opportunities for remuneration are protected.

114. States parties should ensure that appropriate enforcement mechanisms are in place and support children, parents and caregivers in gaining access to the protections that apply.[57] They should legislate to ensure that children are protected from harmful goods, such as weapons or drugs, or services, such as gambling. Robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements.

115. Considering States' obligations to investigate, prosecute and punish trafficking in persons, including its component actions and related conduct, States parties should develop and update anti-trafficking legislation so that it prohibits the technology-facilitated recruitment of children by criminal groups.

116. States parties should ensure that appropriate legislation is in place to protect children from the crimes that occur in the digital environment, including fraud and identity theft, and to allocate sufficient resources to ensure that crimes in the digital environment are investigated and prosecuted. States parties should also require a high standard of cybersecurity, privacy-by-design and safety-by-design in the digital services and products that children use, to minimize the risk of such crimes.

B. Administration of child justice

117. Children may be alleged to have, accused of or recognized as having infringed, cybercrime laws. States parties should ensure that policymakers consider the effects of such laws on children, focus on prevention and make every effort to create and use alternatives to a criminal justice response.

118. Self-generated sexual material by children that they possess and/or share with their consent and solely for their own private use should not be criminalized. Child-friendly channels should be created to allow children to safely seek advice and assistance where it relates to self-generated sexually explicit content.

119. States parties should ensure that digital technologies, surveillance mechanisms, such as facial recognition software, and risk profiling that are deployed in the prevention, investigation and prosecution of crimes are not used to unfairly target children suspected of

[57] General comment No. 16 (2013), para. 37.

or charged with criminal offences and are not used in a manner that violates their rights, in particular their rights to privacy, dignity and freedom of association.

120. The Committee recognizes that, where the digitization of court proceedings results in a lack of in-person contact with children, it may have a negative impact on rehabilitative and restorative justice measures built on developing relationships with the child. In such cases, and also where children are deprived of their liberty, States parties should provide in-person contact to facilitate children's ability to meaningfully engage with the courts and their rehabilitation.

C. Protection of children in armed conflict, migrant children and children in other vulnerable situations

121. The digital environment can provide children living in vulnerable situations, including children in armed conflict, internally displaced children, migrant, asylum-seeking and refugee children, unaccompanied children, children in street situations and children affected by natural disasters, with access to life-saving information that is vital for their protection. The digital environment can also enable them to maintain contact with their families, enable their access to education, health and other basic services and enable them to obtain food and safe shelter. States parties should ensure safe, secure, private and beneficial access for such children to the digital environment and protect them from all forms of violence, exploitation and abuse.

122. States parties should ensure that children are not recruited or used in conflicts, including armed conflicts, through the digital environment. That includes preventing, criminalizing and sanctioning the various forms of technology-facilitated solicitation and grooming of children, for example, though use of social networking platforms or chat services in online games.

XIII. International and regional cooperation

123. The cross-border and transnational nature of the digital environment necessitates strong international and regional cooperation, to ensure that all stakeholders, including States, businesses and other actors, effectively respect, protect and fulfil children's rights in relation to the digital environment. It is therefore vital that States parties cooperate bilaterally and multilaterally with national and international non-governmental organizations, United Nations agencies, businesses and organizations specialized in child protection and human rights in relation to the digital environment.

124. States parties should promote and contribute to the international and regional exchange of expertise and good practices and establish and promote capacity-building, resources, standards, regulations and protections across national borders that enable the realization of children's rights in the digital environment by all States. They should encourage the formulation of a common definition of what constitutes a crime in the digital environment, mutual legal assistance and the joint collection and sharing of evidence.

XIV. Dissemination

125. States parties should ensure that the present general comment is widely disseminated, including through use of digital technologies, to all relevant stakeholders, in particular parliaments and government authorities, including those responsible for cross-cutting and sectoral digital transformation, as well as members of the judiciary, business enterprises, the media, civil society and the public at large, educators and children, and is made available in multiple formats and languages, including age-appropriate versions.