United Nations A/79/122

General Assembly

Distr.: General
9 July 2024

Original: English

Seventy-ninth session
Item 67 (a) of the preliminary list*
Promotion and protection of the rights of children

Sale, sexual exploitation and sexual abuse of children

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children, Mama Fatima Singhateh, submitted in accordance with Human Rights Council resolution 52/26.

* A/79/50.

24-12520 (E) 180724

Report of the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children, Mama Fatima Singhateh

Summary

In the present report, submitted pursuant to Human Rights Council resolution 52/26, the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children, Mama Fatima Singhateh, presents a thematic report on existing and emerging threats that technologies pose to children in facilitating, heightening and committing various manifestations of sale, sexual exploitation and sexual abuse against children, with a view to providing concrete recommendations in line with international standards that would contribute to responding to this problem.

I. Introduction

1. In the present report, the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children examines the misuse of existing and emerging technologies that exacerbate and amplify children's exposure to risks, harms and all forms of sale, sexual exploitation and sexual abuse, with a view to providing concrete recommendations that would contribute towards preventing and responding to this scourge. She also aims to further build on the work of the mandate.[1]

2. To inform the preparation of her report, the Special Rapporteur sought contributions from Member States, international and regional organizations, United Nations agencies, national human rights institutions, law enforcement agencies, civil society and hotline organizations, academics, lawyers, policy experts, child protection officers, educators, communities and children on the existing challenges, as well as practical examples towards addressing this phenomenon.[2] She received over 65 submissions and wishes to thank all stakeholders for their cooperation.

3. The Special Rapporteur also expresses her appreciation for the valuable participation of children and youth advisory members of the Childfund Alliance, Child Right Connect, Terre des hommes, Hintalovon Child Rights Foundation and GlobalChild Program of Research of the University of New Brunswick. She engaged with many children and young people across the globe and would like to extend her deepest gratitude for their meaningful inputs and insight.

II. Activities undertaken by the Special Rapporteur

4. Information on the activities undertaken by the Special Rapporteur since her report to the Human Rights Council dated 5 January 2024[3] is presented below.

5. During the reporting period, the Special Rapporteur transmitted 29 communications jointly with other mandate holders.[4] The full list of press releases and statements issued is available on the mandate holder's webpage.[5]

6. On 5 March 2024, the Special Rapporteur presented the above-mentioned report on child sexual abuse and exploitation in the entertainment industry to the Human Rights Council at its fifty-fifth session.

7. On 6 March, the Special Rapporteur delivered a guest lecture at the University of Lucerne, Switzerland, on her role as a mandate holder, as part of their course on the ethics of human rights.

8. On 7 March, the Special Rapporteur visited the ETH AI Centre in Zürich, Switzerland, and met with academics and experts on their respective projects.

9. On 16 May, the Special Rapporteur participated virtually in a regional advocacy event held in Nepal, organized by End Child Prostitution and Trafficking (ECPAT) International, on engaging the entertainment industry to protect children from sexual exploitation and abuse.

[1] See A/HRC/28/56; A/HRC/12/23; E/CN.4/2005/78/Corr.1; and E/CN.4/2005/78/Corr.2.
[2] See www.ohchr.org/en/calls-for-input/2024/call-input-existing-and-emerging-sexually-exploitative-practices-against.
[3] A/HRC/55/55.
[4] See https://spcommreports.ohchr.org/TmSearch/Mandates?m=288.
[5] See www.ohchr.org/en/latest?field_content_category_target_id%5B158%5D=158&field_content_category_target_id%5B162%5D=162&field_content_category_target_id%5B161%5D=161&field_content_category_target_id%5B159%5D=159&field_entity_target_id%5B1294%5D=1294.

10. From 27 to 31 May, the Special Rapporteur participated in a regional workshop in Senegal, organized by ECPAT International, to share experiences and lessons learned in the fight against child sexual abuse and exploitation in West and Central Africa.

11. On 6 June, the Special Rapporteur launched a youth human rights challenge entitled "Gen Z's take on technology-facilitated child sexual abuse and exploitation".[6]

12. The Special Rapporteur highly appreciates the acceptance of her request from the Government of Germany to conduct an official country visit from 14 to 25 October 2024, and looks forward to a constructive dialogue.

13. The Special Rapporteur would also like to thank the Government of United Arab Emirates for the invitation extended to her to conduct a country visit in the first quarter of 2025.

III. Existing and emerging sexually exploitative practices against children in the digital environment

A. Prevalence of technology-facilitated child sexual abuse and exploitation

14. While existing and emerging forms of technology offer a wide array of opportunities to protect and uphold children's rights, its rapid, evolving and unprecedented capabilities present significant risks.[7] One in three Internet users worldwide are estimated to be children, with a child going online for the first time every half a second.[8] Children today are spending more time in the digital environment than ever before. Almost 80 per cent of children and young people aged 15 to 24 are driving the force of connectivity globally, compared with 65 per cent of the rest of the population.[9] Although access does not determine the value that children derive from technologies, a review of numerous research and reports have revealed the sustained threat and intensification of manifestations of child sexual abuse and exploitation in the digital environment, both in terms of scale and method.[10]

15. In a study, the Childlight Global Child Safety Institute estimates that approximately 302 million children worldwide have been victims of online sexual exploitation and abuse in the past year.[11] The study revealed 12.6 per cent of the world's children have been victims of non-consensual communication, as well as non-consensual sharing of and exposure to sexual images and video.[12] Furthermore, 12.5 per cent of the world's children have been subjected to online solicitation.

16. Survey results from #MyVoiceMySafety poll[13] conducted by the Office of the Special Representative of the Secretary-General on Violence Against Children and WeProtect Global Alliance revealed that 8 in 10 children think it is "likely" or "very likely" for children to experience things that may harm them or make them feel unsafe

[6] See www.ohchr.org/en/special-procedures/sr-sale-of-children/1st-youth-human-rights-challenge.
[7] Office of the United Nations High Commissioner for Human Rights (OHCHR), "UN expert alarmed by new emerging exploitative practices of online child sexual abuse", 5 February 2024.
[8] International Telecommunication Union (ITU), *Guidelines for Industry on Child Online Protection* (Geneva, 2020).
[9] ITU, *Measuring Digital Development: Facts and Figures 2023* (Geneva, 2023).
[10] See submissions from Ombudsman for Children Sweden, Anti-Slavery Australia, El Salvador, Switzerland, Dayananda Sagar University Bangalore and #MyImageMyChoice.
[11] Childlight - *Global Child Safety Institute, Into the Light Index of Child Sexual Exploitation and Abuse Globally: 2024 Report* (Edinburgh, 2024).
[12] University of Edinburgh, "Scale of online harm to children revealed in global study", 28 May 2024.
[13] See www.weprotect.org/youth-consultation-survey.

online, with 45 per cent of respondents perceiving sexual exploitation as the most significant risk when meeting new people online.

17. Research from the Disrupting Harm project[14] shows up to 20 per cent of Internet-using children surveyed in low- and middle-income countries said they had experienced online sexual exploitation or abuse over the past year across 12 countries in Eastern and Southern Africa and South-East Asia.[15] Around one in three children did not tell anyone, and in most countries the perpetrator was someone the child already knew. Among those who did tell, most spoke to their friends, and very few turned to formal reporting mechanisms such as relevant authorities or helplines. Other population-based surveys from high-income countries show that one in five young people experience unwanted online exposure to sexually explicit material, and one in nine young people experience online sexual solicitation.[16]

18. The volume of child sexual abuse materials has grown exponentially since 2010, when there were fewer than 1 million reports.[17] According to the International Centre for Missing and Exploited Children, reports of suspected child sexual exploitation and abuse rose more than 12 per cent in 2023 from the previous year, surpassing 36.2 million reports and containing more than 105 million data files.[18] Alarmingly, reports of self-generated child sexual abuse materials[19] of 7- to 10-year-olds increased by 360 per cent between 2020 and 2022.[20]

19. It is interesting to note that, between 1 August and 31 December 2023, Meta removed more than 90,000 accounts from its platforms.[21] Yet, according to contributions received, around 100,000 child users of Facebook and Instagram are exposed to online sexual harassment every day,[22] including pictures of adult genitalia.[23] This is exacerbated by algorithmic recommendations, hashtags and suggested accounts with which perpetrators can connect.[24]

20. In some cases, technology platforms and online service providers do not have an effective local presence in each jurisdiction in which they provide their services, making information and localized data-sharing, cooperation and/or enforcement ineffective or impossible.[25] The performance and implementation of child-friendly user strategies and policies differ for children in countries from the Global South compared with the Global North.[26] Noticeably, in Australia, the eSafety Commissioner initiated civil penalty proceedings against X (formerly Twitter) for

[14] See www.end-violence.org/disrupting-harm.
[15] See submission from United Nations Children's Fund (UNICEF).
[16] World Health Organization (WHO), "Violence against children online: what health systems and health care providers can do", June 2022.
[17] End Violence against Children, "EU's proposed new legislation promises brave new (online) world", 23 June 2022.
[18] National Centre for Missing and Exploited Children, "2023 CyberTipLine report", 2024.
[19] An alternative term has yet to be agreed under international standards. The present report uses the term "self-generated child sexual abuse materials" with the clarification that the use of this term is not intended to impose any degree of blame or responsibility on the victim-survivor for any abuse or exploitation they experience in connection with the act.
[20] Internet Watch Foundation, "20,000 reports of coerced 'self-generated' sexual abuse imagery seen in first half of 2022 show 7- to 10-year-olds", 8 August 2022.
[21] See submission from Meta.
[22] See submission from Partners for Transparency.
[23] Katie McQue, "Meta documents show 100,000 children sexually harassed daily on its platforms", *The Guardian*, 18 January 2024.
[24] Child Law International Alliance, "An international perspective: addressing challenges to protect children's rights from online sexual exploitation in the digital era", 10 January 2024.
[25] See submission from NetSafe New Zealand.
[26] See submission from Alana.

allegedly neglecting child abuse content[27] and in 2023 issued a formal warning to Google for reportedly failing to manage harmful content detrimental to children.[28]

21. Perpetrators continue to find new and advanced methods to crack and penetrate platforms and services, while hiding their digital footprint. Law enforcement agencies are fighting against this tide, including clamping down on "digital pathways" and "breadcrumbs" used to inform criminal networks and signpost other perpetrators. This public health emergency underscores the urgent need for non-negotiable action and full compliance of child-centric, gender-sensitive and human rights-based due diligence and regulation over content moderation, distribution and amplification of existing and emerging technologies. Just as safety protocols and standards governing other industries have kept members of the general public safe, technological product development should also be mandated to ensure accountability.[29]

B. Relevant international human rights standards

22. The Convention on the Rights of the Child establishes the minimum standards and overarching principles by which every society should treat every child, founded on the principles of non-discrimination (art. 2), the best interests of the child (art. 3), the right to life, survival and development (art. 6) and respect for the views of the child (art. 12).

23. The Convention, inter alia, stipulates that States parties must protect children from all forms of sexual exploitation and sexual abuse, including inducement or coercion to engage in any unlawful sexual activity, the exploitative use of children in prostitution or other unlawful sexual practices and the involvement in pornographic performances and materials (art. 34); prevent the abduction of, sale of or traffic in children for any purpose or in any form (art. 35); and protect children from all forms of exploitation prejudicial to any aspects of the child's welfare (art. 36). The same rights applicable offline must be protected in the digital environment, as affirmed by the General Assembly.[30]

24. The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography also requires State parties to prohibit and criminalize acts stipulated under articles 2 and 3 of the Convention, whether such offences are committed domestically or transnationally or on an individual or organized basis. The diverse forms of abuse are further complemented by the terminology guidelines for the protection of children from sexual exploitation and sexual abuse, which caters for legal definitions and classification gaps.[31]

25. In its general comment No. 13 (2011) on the right of the child to freedom from all forms of violence, the Committee on the Rights of the Child noted that child protection risks in relation to information and communications technology (ICT) comprise the overlapping areas of: (a) sexual abuse of children to produce both visual and audio child abuse images facilitated by the Internet and other ICT; (b) the process of taking, making, permitting to take, distributing, showing, possessing or advertising indecent photographs or pseudophotographs ("morphing") and videos of children and those making a mockery of an individual child or categories of children. The Committee, inter alia, notes that children as users of ICT are also: (a) recipients of information that may expose them to actual or potentially harmful content; (b) in contact with others through technologies,

[27] Australia, eSafety Commissioner, "eSafety initiates civil penalty proceedings against X Corp.", 21 December 2023.

[28] Australia, eSafety Commissioner, "Formal warning: under section 58 on the *Online Safety Act 2021* (Cth)", 3 October 2023.

[29] See submission from University of Lucerne.

[30] See General Assembly resolution 77/320; and Human Rights resolution 32/13.

[31] Susanna Greijer and Jaap Doek, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (Bangkok, ECPAT International, 2016).

which makes then vulnerable to harassment, stalking (child "luring"), grooming, coercion and/or meeting strangers offline for involvement in sexual activities.

26. In its general comment No. 25 (2021) on children's rights in relation to the digital environment, the Committee provides that States should ensure that digital service providers engage actively with children, applying appropriate safeguards, and give the views of children due consideration when developing products and services. This is also in line with article 12 of the Convention, which provides for the meaningful participation of children in all matters affecting them and for their views to be given due weight in accordance with their age and maturity.

27. 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. Under the Guiding Principles on Business and Human Rights and the Children's Rights and Business Principles, all businesses have a responsibility to identify, assess and address human rights impacts, as well as carry out human rights due diligence on their own operations and those in their value chains (even if they have not contributed to actual or potential human rights impacts), while taking appropriate action and providing remediation through legitimate processes.

28. Also in general comment No. 25, the Committee recommends that States require the business sector to undertake child-rights due diligence, in particular to carry out child-rights impact assessments, as well as 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.

29. Robust age-verification and age-appropriate systems should be designed to prevent children from accessing age-inappropriate and harmful content, as well as to provide low-threshold reporting and support channels for children through the wide dissemination of child-friendly and accessible information, consistent with data protection and safeguarding requirements.

30. As per general comment No. 25, in order for rights to have meaning, States parties should ensure that appropriate and effective remedial judicial and non-judicial mechanisms are widely known and readily available to all children and their representatives. Frameworks should include measures for the identification of, therapy and follow-up care for, and the social reintegration of, children who are victims.

31. It is important to note that, during the preparation of the present report, discussions were ongoing on a convention on countering the use of information and communications technologies for criminal purposes. as well as the forthcoming "pact for the future", including its two outcome documents (the global digital compact and declaration for future generations). The Special Rapporteur provided input on the zero draft of the pact to ensure human rights-based and child-sensitive approaches are integrated, including the implementation of child safeguards and meaningful participation of children.[32]

C. Existing challenges

32. Rapid technological development and change presents opportunities for organized criminal groups, perpetrators and traffickers to move and adapt their modus operandi to target victims.[33]

[32] Mama Fatima Singhateh, Special Rapporteur on the sale, sexual exploitation and sexual abuse of children, letter on the zero draft of the Pact for the Future, 8 February 2024.

[33] See submissions from United Nations Office on Drugs and Crime (UNODC), Dutch National Rapporteur Human Trafficking, Dayananda Sagar University Bangalore and NetSafe New Zealand.

Cybersexual harassment

33. Perpetrators often send unsolicited and unwanted sexual advances, comments, messages and visual materials,[34] via social networking sites and messaging services[35] to children. This form of abuse can also involve the disclosure of personal or identifying details of victims (known as "doxing").[36] The few reporting mechanisms available are not widely shared or known about and are ineffective in identifying perpetrators. In many cases, victims rarely receive adequate responses to their complaints via these applications, and perpetrators simply create new fake accounts to continue cyberstalking, harassing and doxing victims.[37]

Non-consensual image-based abuse

34. Image-based abuses involve the creation, capturing, recording, distribution and/or threat of sharing intimate or sexually explicit materials of victims without their consent.[38] It pervades life in many different guises. Non-consensual image-based abuse may be digitally altered and deepfaked,[39] taken surreptitiously in public or private settings without the victim knowing (including "upskirting" and "downblousing") or obtained through solicitation, grooming or coercion. Abusive intimate partners, traffickers, child sexual abuse perpetrators, hackers and others use this method to maintain power and control over victims.[40]

35. Worryingly, there is an increase of so-called anonymous "expose accounts" on social media and online forum threads that have been trivialized as a form of "visual gossip" among peers to maintain social bonds and gendered recognition.[41] The child's name, age, school and social media accounts are often written among the sexually degrading content that are disseminated, which makes it easier for others to identify and harass victims even more.[42] Children are rarely aware that they are committing a sexual offence. It takes a while before these accounts are reported or removed, but by that time it may have already been shared elsewhere among many other users.

Self-generated child sexual abuse materials

36. While sexual content involving and generated by children in and of itself is not necessarily illegal or wrongful, the issue is complex and needs careful attention. This practice often ranges from a product of youth peer pressure, exploration of sexual development or consensual sexting among peers, to coercive grooming and sextortion.[43]

37. The potential for sexual content to spread in the digital environment and offline, from private to public, in a range of settings and recurring forms, beyond and against the will of the child, can make it very difficult to track and remove. This is one of the

[34] See submission from ECPAT Sweden.
[35] Elizabeth Reed and others, "Cyber sexual harassment: prevalence and association with substance use, poor mental health, and STI history among sexually active adolescent girls", *Journal of Adolescence*, vol. 75 (August 2019).
[36] See A/77/302.
[37] See submissions from ECPAT Sweden and Plan International.
[38] United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women) and WHO, "Technology-facilitate violence against women: taking stock of evidence and data collection", March 2023.
[39] See Submission from University of Toronto.
[40] Sophie Maddocks, "Image-based abuse: a threat to privacy, safety, and speech", Media Wellm 15 March 2023.
[41] Katrine Bindesbøl Holm Johansen, Bodil Maria Pedersen and Tine Tjørnhøj-Thomsen, "Visual gossiping: non-consensual 'nude' sharing among young people in Denmark", *Culture, Health and Sexuality*, vol. 21, No. 9 (2019).
[42] See submission from ECPAT Sweden.
[43] See submission from United Nations Interregional Crime and Justice Research Institute (UNICRI).

most dominant types of child sexual abuse materials and reportedly spreads through social media networks, gaming platforms, instant messaging applications, free pornography sites, escort sites, sites for live-streamed webcam sex and other commercial sites.[44]

38. More than 9 in 10 children – including those under the age of 10 – are increasingly being targeted, tricked, groomed, manipulated, blackmailed and coerced into producing and sharing sexual materials of themselves to perpetrators.[45] New data from the Internet Watch Foundation shows that more than 1 in 5 (21 per cent, or 54,250 webpages) of the sites investigated containing "self-generated" imagery contain the most severe abuse, known as category A (including penetration, bestiality and sexual torture), which are being shared widely by perpetrators on dedicated child sexual abuse sites and forums.[46]

39. A recent investigation by the Stanford Internet Observatory identified large networks of accounts on social media openly advertising and trading self-generated child sexual abuse material, with information exchange, keyword searches, hashtags, gift card-related transactions and user suggestion recommendation systems facilitating connections between buyers and sellers.[47] According to the Observatory, this commercialization often replicates the pattern of legitimate independent adult content production, posting content "menus" for imagery of various acts, the curation of networks of followers and fans of an adult performer and content packs for customized offerings. Accounts can also advertise more dangerous services, such as in-person sexual encounters or media depicting bodily self-harm.

40. Furthermore, the likelihood that a child will be held liable for sexual content they created under duress, rather than be seen as a victim, is a cause for concern. The Committee stressed that if such materials are produced as a result of coercion, blackmailing or other forms of undue pressure against the will of the child, those who made the child produce such content should be brought to justice. If such images are subsequently distributed, disseminated, imported, exported, offered or sold as child sexual abuse material, those responsible for such acts should also be held criminally liable.[48] In its general comment No. 25, the Committee states that children should not be held criminally liable for possessing or producing images of themselves solely for their own private use. When it comes to the growing trend of peer-to-peer violence, States should focus on prevention and make every effort to create and use alternative methods to a criminal justice response.

Sexual extortion of children

41. Social media platforms, chatrooms and gaming networks are a starting point for many recruitments.[49] Conversations with children can escalate into high-risk grooming situations as quickly as 19 seconds from the first message, the average grooming time being just 45 minutes.[50] Perpetrators often employ a combination of tactics and psychological manipulation to befriend, flatter, lure and coerce child victims in gaining their trust; sharing personal information or explicit content; engaging in relationships or role-play games that involve sexual activities; or offering

[44] See submission from Ombudsman for Children in Sweden.
[45] Internet Watch Foundation, "'Self-generated' child sexual abuse", IWF annual report 2023. Available at www.iwf.org.uk/annual-report-2023/trends-and-data/self-generated-child-sex-abuse/.
[46] Internet Watch Foundation, "Under 10s groomed online 'like never before' as hotline discovers record amount of child sexual abuse", 17 January 2024.
[47] Stanford Internet Observatory, "Cross-platform dynamics of self-generated CSAM", 7 June 2023.
[48] See CRC/C/156.
[49] See submissions ECPAT Belgium and Defence for Children International.
[50] WeProtect Global Alliance, *Global Threat Assessment 2023* (2023).

money or virtual in-game currency in exchange for sexual activity; among other forms of exploitation.[51]

42. Global law enforcement, including the Federal Bureau of Investigation of the United States of America, the Royal Canadian Mounted Police, the National Crime Agency of the United Kingdom of Great Britain and Northern Ireland and the New Zealand Police, issued a public safety alert over the rapid increases in financial "sextortion" crimes targeting children, which bear the hallmarks of organized crime,[52] noting shifts in patterns of behaviour, motivation and scripts by criminals and gangs based in the United States and in West Africa and South-East Asia,[53] thus presenting a new set of multifaceted challenges, including difficulties in enforcement, and jurisdictional and technological hurdles.[54]

43. The number of reports received by the Internet Watch Foundation in the first half of 2023 involving sexual extortion of children increased by 257 per cent compared with the whole of 2022.[55] New data published revealed that teenage boys were most at risk of being targeted for financial motives, while girls appeared to be targeted for more sexually explicit materials.[56] In most cases, perpetrators often create a fake account and initiate conversations with children, pretending to be someone else and having no shared friends in common.[57] They feign romantic interest and, soon after, use the child's sexual images or videos obtained to blackmail or extort them for either money or more sexually explicit materials.[58] Not only does this leave the child constantly in distress over the material's potential circulation or upload, but it also has grave repercussions, including self-harm or suicide.

44. Sometimes, these images or videos are taken without the knowledge of the child or are digitally altered. In the case of boy victims, predators often use fake female accounts or masquerade as teenage girls,[59] while pimps and traffickers use the "lover boy" approach to profile and exploit girls, especially those confronted with economic and social hardship, into sexual exploitation. There is also a risk of incidents moving to in-person grooming and physical meetings at private rental accommodations.[60]

Live streaming of child sexual abuse

45. The live streaming of child sexual abuse is an established reality and poses serious and unique challenges, where demand-side perpetrators hide behind their screen and pay to direct specific acts of degrading treatment and sexual violence against children in real-time by typing in the chatrooms and/or dictating the abuse audibly on the video call instantaneously.[61] This is on par with abusing the children themselves.

---

[51] See submissions from Dayananda Sagar University Bangalor and Safety on Social and Partners for Transparency.

[52] Australian Centre to Counter Child Exploitation, "AFP joins international law enforcement agencies to deliver joint warning about global financial sextortion", 7 February 2023.

[53] United States of America, Federal Bureau of Investigation, "Sextortion: a growing threat targeting minors", 16 January 2024.

[54] Avi Jager and Hezi Jenik, "Online sextortion: rising tides, new motivations, and unique solutions", Active Fence, 28 September 2023.

[55] Internet Watch Foundation, "Hotline reports 'shocking' rise in the sextortion of boys", 18 September 2023.

[56] Internet Watch Foundation, "Teenage boys targeted as hotline sees 'heartbreaking' increase in child 'sextortion' reports", 18 March 2024.

[57] Jager and Jenik, "Online sextortion".

[58] See submissions from UNICRI and International Child Rights Center.

[59] United States of America, Federal Bureau of Investigation, "FBI and partners issue national public safety alert on financial sextortion schemes", 19 December 2023.

[60] See submissions from ECPAT Belgium and Defence for Children International.

[61] See submissions from International Justice Mission and International Child Rights Center.

46. In 2020, the infamous case of "Nth Room", allegedly involving around 260,000 men, monetized the forcing of young women and girls into filming sexually explicit and torturous videos in a series of chat rooms on an instant messaging app to be sold for profit.[62] The fury in public sentiment led to significant legal amendments and tougher penalties within the Republic of Korea.[63]

47. It is possible for the facilitators or perpetrators of sexual abuse and exploitation of children not to be co-located with their victims, either in the same room or the same country.[64] Alarming findings from the Scale of Harm survey reveal that nearly half a million children in the Philippines have been trafficked to produce child sexual exploitation material, often by relatives or people they know.[65] Children from the global South are predominately targeted by male perpetrators, typically from Western or English-speaking countries.[66]

D. Emerging challenges

48. Emerging technologies risk not only replicating existing safety concerns that plague the current digital ecosystem and technological landscape, but also exacerbate and facilitate more severe threats against children if not mitigated.

Artificial intelligence-generated child sexual abuse materials

49. Technologies such as deepfakes, nudifying, de-aging, artificial intelligence embedded peer-to-peer file sharing and voice cloning continue to amplify and extend existing methods being used for malicious purposes to exploit children and produce child sexual abuse materials.[67] More than 96 per cent of pornography generated by artificial intelligence was produced without the consent of the individual featured.[68]

50. Generative artificial intelligence can be weaponized through several techniques, namely: (a) text-to-image models where users type in a description (also known as a prompt) of the image they wish the artificial intelligence to produce, including featuring preferred settings, individuals, styles, positions or activities; (b) image-to-image models, where images and text prompts are used as an input or a basis to create new artificial intelligence-generated child sexual abuse materials; and (c) inpainting, which is an image-to-image technique that allows users to dictate the specific areas of a real image they wish to change, down to the finest detail.[69] Little to no interaction with children is needed, and material can be easily accessible and downloaded offline, leaving companies and law enforcement in the dark with no opportunity of oversight.[70]

51. These methods act as a gateway for perpetrators either to adapt and customize original child sexual abuse materials into new content, to produce and manipulate accessible and benign content of known or unknown children (also content of interest

[62] Asia Pacific Forum on Women, Law and Development, Korea women's Association United and Korea Centre for United Nations Human Rights Policy, joint stakeholder report prepared for the forty-second session of the 4th Universal Periodic Review Working Group of Republic of Korea, March 2023.
[63] See submission from International Child Rights Center.
[64] See submission from International Justice Mission.
[65] International Justice Mission and University of Nottingham Rights Lab, *Scale of Harm Research Method, Findings, and Recommendations: Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines* (2023).
[66] See submission from International Justice Mission.
[67] See submissions from the International Centre for Missing and Exploited Children and University of Toronto.
[68] See A/HRC/56/48.
[69] See submission from UNICRI.
[70] See submissions from UNODC and Anti-Slavery Australia.

to predators)[71] into sexually abusive material, or even to create fully artificial intelligence-generated child sexual abuse materials from scratch.[72] Such material can be realistic and convincing enough to be indistinguishable from real images, videos and audio of child sexual abuse and exploitation, or can look like synthetic and non-photographic images and videos of child sexual abuse and exploitation, such as cartoons or drawings.

52. Perpetrators also exploit the ability of artificial intelligence to generate technological know-how and information on how to commit such crimes, to mimic natural human language and offer behavioural tips, allowing them to groom children in automated and more targeted ways,[73] and to cover up and avoid prosecution by coercing victims and tampering with evidence.[74]

53. In 2023 alone, the International Centre for Missing and Exploited Children received 4,700 reports of content generated by artificial intelligence that depicted child sexual exploitation and abuse (a category it only started tracking in 2023).[75] During a one-month period of initial investigations, the Internet Watch Foundation uncovered 11,108 artificial intelligence-generated images posted on a dark-web forum that were deemed most likely to be criminal and depicting children, including babies, toddlers and primary school-aged children.[76] The Foundation further sounded the alarm on 51 URLs processed in 2023 containing actionable artificial intelligence-generated images of child sexual abuse, of which 42 looked like "real" images.[77] Analysts from the Foundation noted the difficulty with hashing artificial intelligence-generated child sexual abuse materials in comparison to traditional forms.[78]

54. In a study by Stanford Internet Observatory, LAION-5B – a data set of 5 billion images – was found to have contained over 1,000 URLs containing child sexual abuse materials.[79] This data set and other related data sets have been used to train notable artificial intelligence platforms and image generators, such as Stabel Diffusion and Google's Imagen. Without strict monitoring and access to data sets used to train these artificial intelligence models, it is impossible to prove that no actual harmful sources or child sexual abuse materials are being used.[80] The quality of output of artificial intelligence models has the potential to improve further and generate more lifelike materials, which will enable realistic full-motion video content to become commonplace. The Internet Watch Foundation has reportedly seen the first examples of short artificial intelligence-generated child sexual abuse videos.[81]

55. In turn, this will affect the detection and prioritization of cases by law enforcement, making it increasingly difficult to triage, distinguish and identify victims, identify whether or not there is a real child in danger, or identify whether certain elements have been tampered with (such as if the places or acts portrayed are

[71] Resolver, "COITP: how predators hide in plain sight", 28 September 2023.
[72] See submissions from University of Toronto, Child Rights International Network and ECPAT Sweden.
[73] See submissions from eSafety.
[74] Thorn, "Thorn and All Tech is human forge generative AI principles with AI leaders to enact strong child safety commitments", 23 April 2024.
[75] See submission from the International Centre for Missing and Exploited Children.
[76] Internet Watch Foundation, "How AI is being used to create child sexual abuse imagery" October 2023.
[77] Internet Watch Foundation, "AI generated child sexual abuse", IWF annual report 2023. Available at www.iwf.org.uk/annual-report-2023/trends-and-data/ai-generated-child-sexual-abuse/.
[78] Internet Watch Foundation, "How AI is being used to create child sexual abuse imagery".
[79] Stanford Internet Observatory, "Identifying and eliminating CSAM in generative ML training data and models", 23 December 2023.
[80] See submissions from the International Centre for Missing and Exploited Children and its Australia office.
[81] Internet Watch Foundation, "How AI is being used to create child sexual abuse imagery".

real).[82] This could lead potential investigators to spend time and resources pursuing the rescue of children who may turn out to be virtual characters, or waiting for further verification of the quality of the content generated. Crucially, legal issues arise in many countries as to the legal status of artificial intelligence models, the production of artificial intelligence-generated child sexual abuse materials[83] and the creation of guides to utilize artificial intelligence to generate child sexual abuse materials, which may not be criminalized as offences.[84]

56. The sheer volume and circulation of this type of material often allow perpetrators to commercialize and profit from bespoke content and drives down the prices of child sexual abuse material, possibly leading perpetrators to produce more.[85] It is sometimes sponsored through paid advertisement on platforms[86] and easily found through highly ranked websites on leading search engines.[87]

57. Generative artificial intelligence is falsely promoted as a "harm-free" approach, similar to when perpetrators claim that viewing child sexual abuse material is not detrimental since it already exists and its "just a picture" or "fantasy", as they are not actively contacting children and/or creating new materials.[88] Contrary to this view, research conducted found that 52 per cent of respondents felt afraid that viewing child sexual abuse materials might lead to sexual acts against a child, 44 per cent said that viewing child sexual abuse materials made them think about seeking contact with a child, and 37 per cent said they had sought direct contact with a child after viewing child sexual abuse material.[89]

58. Artificial intelligence-generated child sexual abuse material is not simply "made up", but a response to intentionally sought out technological curation. It perpetuates a culture of violence and can lead to desensitization. Debates around its tangibility should not diminish the severity and real impact on victims and survivors.[90]

Extended reality technologies

59. As this consumer market continues to grow rapidly in popularity worldwide (with the potential to reach £1.4 trillion by 2030),[91] extended reality technology creates new ways for perpetrators to gain access to, stream images of, exploit and sexually abuse children, especially when there are no legal restrictions or robust age assurance measures.[92] It merges the virtual and real world to create material that is more intrusive and hyperrealistic, with an enhanced impact on the senses, including touch, sight and others.[93] The year 2024 started with deeply concerning news that police in the United Kingdom were reportedly investigating an alleged gang-rape by several adult men of a child's avatar in a virtual reality game.[94]

---

[82] See submission from Anti-Slavery Australia.
[83] See submission from the International Centre for Missing and Exploited Children.
[84] Internet Watch Foundation, "How AI is being used to create child sexual abuse imagery".
[85] See submission from UNODC.
[86] See submission from Alana.
[87] Clare McGlynn, "New: deepfake nudes and why Google must act", 4 October 2023.
[88] See submissions from the International Centre for Missing and Exploited Children and Suojellaan Lapsia.
[89] Suojellaan Lapsia, *CSAM Users in the Dark Web: Protecting the Children through Prevention* (2021).
[90] See submission from International Child Rights Center.
[91] PWC Indonesia, "Virtual and augmented reality could deliver a £1.4 trillion boost to the global economy by 2023 – PWC", 2020.
[92] WeProtect Global Alliance, "Extended reality technologies and child sexual exploitation and abuse", 28 February 2023.
[93] See submissions from eSafety, Virtual Reality Risks Against Children, ECPAT International and ODI.
[94] Iain Drennan, "Virtual reality risks to children will only worsen without coordinated action", WeProtect Global Alliance, 3 January 2024.

60. Research by the Centre for Countering Digital Hate found that users, including children, were exposed to abusive behaviour, such as graphic pornographic and sexual content, bullying, sexual harassment, grooming and racism, every seven minutes.[95] Perpetrators present themselves through child-like avatars or filters and use "private spaces" to interact and deepen their relationships with children, as well as distribute child sexual abuse materials among networks without being heard or seen.[96] Some applications allow users to create indecent synthetic images by creating their own fantasy characters or scenarios.[97] Other legitimate games allow users to venture outside and explore real locations, presenting contact risks and opportunities for in-person grooming.

Cryptocurrency-based sale of child sexual abuse materials

61. Virtual currencies are almost exclusively the dominant choice for payment for abuse materials, as they provide anonymity[98] and evade traditional financial institutions and law enforcement detection, thus making it difficult to trace and track illicit transactions.[99] In 2023, the Internet Watch Foundation investigated 2,809 reports of commercial sites offering a payment option for child sexual abuse material, including 845 instances where cryptocurrencies were offered as payment option, attributed to 332 unique URLs.[100]

62. Moreover, in 2023, the Special Rapporteur on contemporary forms of slavery, including its causes and consequences noted that cryptocurrencies are also used by perpetrators to purchase Internet domains and other platforms to recruit victims and clients, and by customers to purchase premium memberships on review board websites previously used to trade sexual abuse materials.[101] Research by Chainalysis found that sellers of child sexual abuse materials are using privacy tools like "mixers" and "privacy coins" that obfuscate their money trails across blockchains.[102] The lifespan of the average active vendor in 2023 was 884 days, in contrast to 560 days the previous year.

End-to-end encryption

63. It is undeniable that time-limited disappearing messages, anonymization[103] and end-to-end encryption technologies that lack built-in child safety mechanisms shield criminal activities by bypassing conventional monitoring systems.[104] Research conducted by Suojellaan Lapsia – which surveyed over 30,000 active online child sexual offenders – revealed that end-to-end encrypted messaging apps are being used to search for, view and share child sexual abuse materials.[105] This is often preferred by perpetrators owing to the perceived security and privacy offered, as it conceals

[95] Centre for Countering Digital Hate, "Facebook's metaverse", 30 December 2021.
[96] See submission from Virtual Reality Risks Against Children.
[97] WeProtect Global Alliance, "Extended reality technologies and child sexual exploitation and abuse".
[98] Financial Coalition against Child Pornography and International Centre for Missing and Exploited Children, "Cryptocurrency and the blockchain: technical overview and potential impact on commercial child sexual exploitation", May 2017.
[99] See submissions from Dayananda Sagar University Bangalore; Mulier; Anti-Slavery Australia.
[100] Internet Watch Foundation, "Commercial content", IWF annual report 2023. Available at www.iwf.org.uk/annual-report-2023/trends-and-data/commercial-content/.
[101] A/78/161.
[102] Chain Analysis, "CSAM and cryptocurrency: on-chain analysis suggests CSAM vendors may benefit from privacy coins like Monero and other obfuscation measures", 11 January 2024.
[103] See submission from NetSafe New Zealand.
[104] See submissions from Plan International and Anti-Slavery Australia.
[105] Suojellaan Lapsia, "Tech platforms used by online child sexual abuse offenders", February 2024.

their identities and involves a closed channel of communication between the sender and receiver.[106]

64. Without effective surveillance or a law enforcement presence, perpetrators are able to mask all traces of their activities, exchange sensitive information, negotiate prices and coordinate logistics with a minimal digital footprint,[107] resulting in limited data-sharing, wilful blindness to illegal activities and unwanted obstacles towards combating this phenomenon.[108]

65. Despite warnings, some technology companies have taken the extraordinary step of rolling out end-to-end encryption, which will have a catastrophic impact on law enforcement's ability to identify child victims and bring perpetrators to justice.[109] When analysing the International Centre for Missing and Exploited Children's 2023 volume of reports of suspected child sexual abuse materials, there is a notable contrast between those employing end-to-end encryption and those that do not. Contributions received show that WhatsApp, which employs end-to-end encryption, reported 1,389,618 instances of child sexual abuse, while Facebook and Instagram, which do not (prior to launching default end-to-end encryption) reported 17,838,422 and 11,430,007, instances respectively.[110]

66. Evidently, the discussion surrounding encryption technologies merits careful consideration.[111] While some methods have been proposed to provide an alternative "back door" into end-to-end encrypted channels,[112] they have been deemed ineffective because they defeat the inherent mathematical design properties of end-to-end encryption, as a result reducing the integrity and security of services.[113] From the perspective of privacy advocates, law enforcement agencies already have access to technology-based investigative techniques that do not require the breaking of encryption, where they can obtain a warrant to seize the devices of particular suspects or look at the metadata of communications.[114] There is concern that, if encryption were completely removed, this could leave children, especially those from vulnerable or marginalized groups, susceptible to a wide range of abuse, policing, surveillance, intelligence-gathering or other intrusive data practices.[115]

67. Against this backdrop, end-to-end encryption cannot be addressed in isolation, as safety, privacy, security and child protection concerns are a part of the wider digital ecosystem.[116] An inclusive, balanced, human rights-based, intersectional and child-rights approach must be factored into the discourse, as children are a diverse group of rights-holders – with the rights to protection, privacy, non-discrimination, life, health and freedom of expression – and the impact of encryption can vary significantly depending on their age, maturity, background, experiences, perspectives, needs and identities. While being mindful of techno-solutionism, each concern can be

[106] See submissions from Suojellaan Lapsia and SLSN.

[107] See submissions from Malaysia, Montenegro, Slovenia, Suojellaan Lapsia, Plan International, ECPAT International, ECPAT Sweden, NetSafe, University of Toronto, Dayananda Sagar University Bangalore, Maat for Peace and Symbiosis Law School.

[108] See submissions from ECPAT International and NetSafe.

[109] Virtual Global Taskforce, "Technological tipping point reached in fight against child sexual abuse", January 2024.

[110] See submission from Terre des Hommes.

[111] See submissions from Suojellaan Lapsia, Privacy International and Child Rights International Network.

[112] Donagh O'Malley, "Child safety and end-to-end encryption: irreconcilable or a possible match?", WeProtect Global Alliance, 31 May 2023.

[113] See submissions from Estonia and Privacy International.

[114] Child Rights International Network and Defend Digital Me, *Privacy and Protection: A Children's Rights Approach to Encryption* (2023).

[115] See submission from Child Rights International Network.

[116] See submissions from eSafety and Child Rights International Network.

addressed through the meaningful participation of children, as well as the thoughtful and intentional design and supervision of technologies taking into account societal problems affecting all children.[117]

"Kidfluencing" and "sharenting" accounts

68. Alarmingly, parental figures are some of the main producers of sexual content involving pre-pubescent children, in particular girls.[118] The wilful lack of attention paid by those who manage child influencer and "sharenting" accounts – typically parents/caregivers, who also assume responsibility for the filming, editing, production and posting of content, and for facilitating business relationships – adds another complex layer to a $24 billion industry that is led by influencer agencies, advertising agencies, brand managers, etc.[119] Children in this context are commodified, framed, appropriated for postings and advertorials, resulting in branded childhood and private requests.[120] Much of this child content is not available, but instead provided privately either through paid subscriptions and/or for a one-time fee.[121]

69. The volume of traffic clearly demonstrates the scale of demand for the sexualization of children for perpetrators' own sexual gratification,[122] as well as potentially operating as a "storefront" for the sale, sexual abuse and exploitation of children on demand.[123] Such accounts and sites should not be deemed by States, technology companies and online service providers as low-risk just because they are run by parents or caregivers. The Special Rapporteur is concerned that this practice also raises a question about how many images of children from everyday parent/caregiver-run accounts, i.e. not child public figures, influencers, performers, or "sharenting" or "kidinfluencing" accounts, is being collected by criminals to use when creating child sexual abuse materials.

IV. Disproportionate impact on vulnerable and marginalized groups

70. The digital environment reinforces and exacerbates systemic and structural inequalities, intersecting forms of discrimination, deep-seated cultural and social norms, as well as patterns of harmful masculinities.[124] Children belonging to vulnerable and marginalized groups are at greater risk of facing technology-facilitated child sexual abuse and exploitation. Such violence in the digital environment leads to violence offline.[125] The consequences are certainly all too real and can result in short- and long-term social and health effects,[126] including fear, anxiety, depression, social isolation, poor school performance, post-traumatic stress disorder, suicidal thoughts and worse, among others.[127]

---

[117] Ibid.

[118] Michael Salter and Tim Wong, "Parental production of child sexual abuse material: a critical review", *Trauma Violence and Abuse*, vol. 25, No. 3 (July 2024).

[119] See submission from University of Essex and Plataforma Tres Voces por la Paz.

[120] Crystal Abidin, "Micromicrocelebrity: branding babies on the Internet", *M/C Journal*, vol. 18, No. 5 (2015).

[121] House of Commons, Digital, Culture, Media and Sport Committee, "Oral evidence: influencer culture, HC 258", Tuesday 2 November 2021, Q219 (Catalina Goanta).

[122] Jenna Drenten, Lauren Gurrieri and Meagan Tyler, "Sexualized labour in digital culture: Instagram influencers, porn chic and the monetization of attention", *Gender, Work and Organization*, vol. 27, No. 1 (January 2020).

[123] See submission from University of Essex.

[124] See submissions from UNICEF and Terre des Hommes.

[125] See submission from Global Kids Online.

[126] WHO, "What are the consequences of online violence against children?", 10 January 2022.

[127] See www.unfpa.org/thevirtualisreal.

71. The social position of the victim can influence their willingness or accessibility to take legal action, especially those who do not wish to disclose facts about themselves.[128] The outcome of some of the conversations held with children suggests that children believe that law enforcement agencies do not take violence in the digital environment as seriously as violence offline. This also demonstrates the attitudinal barrier that exists on how violence in the digital environment is perceived.[129]

72. In a global study conducted by Economist Impact, 54 per cent of respondents aged 18 to 20 reported they had experienced online sexual harms during their childhood, with most harms happening in private. In total, 68 per cent of respondents had received sexually explicit content through private messaging services, 29 per cent through private image and video-sharing services and 18 per cent through open forum social media.[130] Of the respondents, 65 per cent self-identified as LGBTQ+, 57 per cent self-identified as persons with disabilities and 58 per cent self-identified as an ethnic/racial minority.

73. Technology-facilitated child sexual abuse and exploitation often has gendered implications as it rests on gendered values and social implications, forming the basis for judging girls' and boys' sexual activities differently.[131] Present day hegemonic cultural representation normalizes such behaviours, where boys and young men gain respect and popularity through the possession of unauthorized sexual materials, which become capital and commodities in the digital marketplace to gain access to other children's bodies, while sexual double standards underpin victim-blaming responses to girls and young women whose images and videos are distributed without their consent, and who are subsequently blamed and held responsible for (not preventing) the abuse in the first place.[132]

V. Comprehensive and holistic response to drive needed change

74. Several States have provided examples of efforts being made to drive the change needed to better mobilize and respond to technology-facilitated child sexual abuse and exploitation. These examples include child participation in decision-making processes; undertaking research and pilot projects; adopting specific laws and regulations; providing legal aid and medical care to victims and survivors; adopting national action plans, protocols and strategies; conducting educational and awareness-raising campaigns to promote digital literacy; putting in place parental control mechanisms; establishing response centres and helplines, including anonymous reporting platforms; creating multi-professional teams at schools to provide psychosocial and socio-educational support services to children; and implementing specialized crime prevention units and national referral mechanisms for victims of trafficking, among others.[133]

75. Technology companies and online service providers have an important role to play in driving the change needed to respond to technology-facilitated child sexual abuse and exploitation, yet this role has been largely left to self-regulation and

[128] See submissions from ECPAT Belgium and Defence for Children International.

[129] See also, A/77/302.

[130] WeProtect Global Alliance, "Estimates of childhood exposure to online sexual harms and their risk factors: A global study of childhood experiences of 18 to 20 years olds", 2021.

[131] See submission from ECPAT Sweden.

[132] Marijke Naezer, "Only sluts love sexting: youth, sexual norms and non-consensual sharing of digital sexual images", *Journal of Gender Studies*, vol. 30, No. 1 (2021).

[133] See submissions from Council of Europe, IIN-OAS, Albania, Chile, Colombia, Ecuador, El Salvador, Estonia, Luxembourg, Malaysia Montenegro, Qatar, Russia, Slovenia, Spain and Switzerland.

voluntary approaches by the industry.[134] Efforts brought forward will remain reliant on the goodwill of technology companies and online services providers, unless made mandatory.[135]

Technical and regulatory standards as a baseline

76. It is imperative to mainstream the rights of children within business models, rather than retrofitting safeguards after harm has occurred. Privacy- and safety-by-design approaches ensure that the security and integrity of technological infrastructure are not compromised. In line with the Guiding Principles on Business and Human Rights, businesses and their value chains must integrate robust review mechanisms and safety protection nets to ensure comprehensive child rights due diligence and periodic impact assessments (including of their policies, operations, deployment, algorithms and moderation processes) to assess and minimize actual or potential risks to children, with the implementation of grievance mechanisms and remedial measures.[136]

77. Strengthening the ethics of due process safeguards, transparency and accountability of the industry as a whole makes it possible to pinpoint where weaknesses exist in safety practices; where discrepancies exist in respect of the extent of their action, performance and presence in jurisdictions; what innovative and preventive technologies are needed; and where law enforcement is required.[137] In cases of serious threats of adverse human rights impacts, transparency may require the sharing of code or data sets.[138] Creators of training models and data sets must rectify and implement effective safeguards and filters to supress harmful content.[139]

78. To start with, instead of passively relying on warrants, notices and takedown procedures, the burden to report abuse should be taken away from children and placed back on technology companies and online service providers.[140] Businesses must therefore be mandated to proactively and rapidly implement concrete automated and human (manual) detection, removal and moderation tools, and to promptly report to the relevant authorities any harmful, exploitative and abusive content of children occurring or amplified through their products and services, including by identifying real-time abuse,[141] as well as accounts used by perpetrators.[142]

79. Conversations with children suggested the need for clear instructions on social media platforms on how to report abuse and know what services are available for them, including assurances that their reports will be dealt with promptly. Some children highlighted the complexity of navigating different reporting procedures across different platforms, which can be overwhelming, frustrating and leave some unsure where to turn to for help. Therefore, when designing and engineering technologies, greater choices over content moderation and user-controlled moderation settings should be provided, including robust age verification and restriction; parental controls; regular reminders and notifications of dangers to users; restricting

[134] A/HRC/28/56 and A/HRC/52/61 provide an extensive range of actions undertaken, for which is not repeated in this report.
[135] Equality Now, *Ending Online Sexual Exploitation and Abuse of Women and Girls: A Call for International Standards* (2021), p. 11.
[136] See A/C.3/78/L.19/Rev.1.
[137] See A/HRC/52/61.
[138] United Nations Educational, Scientific and Cultural Organization, “Recommendation on the ethics of artificial intelligence”, 2022.
[139] See submission from the International Centre for Missing and Exploited Children.
[140] See submissions from ECPAT Belgium and Defence for Children International.
[141] See submissions from Ecuador, Defensor de la Niñez, International Justice Mission, Partners for Transparency and NetSafe New Zealand.
[142] See submission from Partners of Transparency.

interactions and making private the follower lists of children; and implementing warning tools and deterrence campaigns to suspected perpetrators. Other necessary measures include providing easy-to-use reporting, blocking and content removal options within the platform, including confidential and anonymous reporting features; and ensuring accessible child-friendly and age-appropriate user safety controls, as well as remedial and appropriate referral channels to relevant law enforcement and child protection authorities and helplines.[143] Such measures must be sensitive to the vulnerabilities, cultural and linguistic needs and circumstances of children.

80. National authorities or regulators should put in place mandatory industry-specific codes that proactively anticipate and enforce child safeguarding across all existing and emerging technologies, especially with respect to the minimizing, restriction and removal of explicit, sexually objectifying and harmful content.[144] Financial regulators and intelligence units should also adopt prescriptive regulations and actionable financial intelligence disclosures to law enforcement agencies on suspicious transactions of child sexual abuse and exploitation, including through virtual currencies.[145] The Special Rapporteur calls for strict criminal liability to be imposed on tech companies, online service providers and/or their value chains for human right violations.

Strengthen investigative and judicial proceedings

81. Due to the borderless nature of the digital environment, perpetrators may choose to operate from jurisdictions that appear as safe heavens with weak legal frameworks that do not capture the full spectrum and gravity of these crimes,[146] or from jurisdictions that lack extradition agreements.[147] Other factors that impede investigative, judicial and reparative proceedings include the lack of recognition of victims and survivors;[148] strict evidence validity and jurisdiction criteria;[149] victims and relatives dealing with complex technical processes, with limited knowledge about their rights and easy reporting mechanisms available;[150] substantial staffing cuts to crucial child protection units across public services;[151] limited resources and pathways to comprehensive ongoing response and support services to victims and survivors;[152] disjointed or imperfect cooperation within and across borders;[153] and little to no access to reparation and compensation schemes for victims and survivors. Strict data privacy regulations and short retention of data by technology providers can also limit the capabilities of law enforcement agencies.[154]

82. It is also worth noting that technological innovations often surpass the capacities of law enforcement and judicial officials, who often lack the financial resources, expertise, specialized training and advanced technology tools in terms of new methods, techniques and trends to guide actions with respect to undercover

[143] See submissions from Colombia, Luxembourg, Spain, NetSafe New Zealand.
[144] See submissions from eSafety, Plataforma Tres Voces por la Paz and ECPAT New Zealand.
[145] See submissions from the International Centre for Missing and Exploited Children and International Justice Mission.
[146] See submissions from Office of the Special Representative of the Secretary-General for Children and Armed Conflict; UNODC, UNICRI, Slovenia and Defensor de la Ninez.
[147] See submission from NetSafe New Zealand.
[148] See submissions from SLSN and ODI.
[149] UNODC, *Exploitation and Abuse: The Scale and Scope of Human Trafficking in South Eastern Europe* (Vienna, 2022).
[150] See submissions from El Salvador and NetSafe New Zealand.
[151] See submission from ECPAT New Zealand.
[152] See submission from NetSafe New Zealand.
[153] See submissions from the International Centre for Missing and Exploited Children, NetSafe New Zealand, ECPAT Belgium, DEI and ODI.
[154] See submissions from Malaysia, Slovenia and SLSN.

operations, computer forensics, victim identification, evidence handling and following financial trails.[155]

83. One of the best practices for effective investigation and prosecution is the creation of specialized multidisciplinary units with sufficient allocated resources, including technical forensic personnel, prosecutors and psychologists specialized in child rights, cybercrimes and forensic interviewing.[156] Artificial intelligence tools can also be leveraged to help at different stages of an investigation workflow. These include preventive and deterrence technologies, content generation, text and speech analysis, image analysis, and process and workflow optimization.[157] This would remove child sexual abuse materials automatically and reduce the need for individuals to be exposed to harmful content during review processes.[158]

84. Given the transnational nature of these offences, it is imperative to respond to this phenomenon through prompt collaboration and accurate responses among regulatory bodies, law enforcement and industry stakeholders across borders.[159] Children want to see effective law enforcement at the national level that is capable of intervening and combatting technology-facilitated abuse, with strict sanctions against perpetrators.[160] A global regulatory standard and methodology would be critical to harnessing the complexities and determining the applicability of different legislative and regulatory frameworks in order to foster standard classification, enhance international justice cooperation, avoid delays and inconsistencies, as well as reduce loopholes and pockets of threats, especially with respect to organized crimes.[161]

Early, comprehensive and inclusive public health approaches

85. The outcome of the conversations with children showed that many of them have access to a support structure from parents, teachers and school counsellors. Yet many admit that they or their peers will not seek help from these structures as they do not feel they have safe spaces to go to, as they fear and worry about the potential consequences of speaking out, including stigmatization and victim-blaming. Some parents find monitoring their children's activities challenging or do not understand privacy setting and application functionalities.[162] Children also identified the need to increase educational and community campaigns, as well as public awareness-raising about the serious nature of technology-facilitated child sexual abuse and exploitation and how to navigate the digital environment safely, including the promotion of healthy and positive sexual behaviour and demystifying the idea that only strangers sexually abuse children. Sensitization must go beyond home and school settings and place the onus on traditional and social media platforms, including online communities, radio, film, television programmes and newspapers, in order to warn wider audiences on potential harms.[163]

---

[155] See submissions from the International Centre for Missing and Exploited Children, ECPAT Belgium, DEI SLSN, Mexican NHRI, Defensor de la Ninez, Plataforma Tres Voces por la Paz, Scottish Biometrics Commissioner, Laura Lisita, Colombia, Montenegro and Luxembourg.

[156] See submissions from the International Centre for Missing and Exploited Children and NetSafe New Zealand.

[157] See submissions from UNICRI, eSafety, International Child Rights Center, ECPAT Belgium and DEI.

[158] See submissions from eSafety and International Child Rights Center.

[159] See submission from Sovereign Order of Malta.

[160] Based on conversations with children within the margins of report preparation.

[161] See submission from Global Online Safety Regulators Network.

[162] See the baseline summary factsheets of Terre des Hommes, available at www.terredeshommes.nl/en/publications/child-friendly-baseline-summary-factsheets-scrol.

[163] See submissions from Office of the Special Representative of the Secretary-General for Children and Armed Conflict and eSafety.

86. Repeated exposure to extreme forms of hypersexualization and pornographic material can have a significant impact on a child's development, leading to trivialization of the phenomenon and distorting what is considered normal sexual interactions.[164] The Special Rapporteur on violence against women and girls, its causes and consequences stressed that the regular exposure of children to pornography has also been linked to the quadrupling of underaged victims of sexual offenses over the past decade, hence creating a demand for an inherently violent system built on the sexual subordination of girls.[165]

87. Comprehensive and long-term public health approaches are vital to transform harmful societal norms, gender masculinities, stereotypes and paternalism at a broader societal level.[166] Such efforts require a range of sufficiently funded, well-coordinated, sustained actions targeted at different levels to respond to immediate and long-term needs which focus on the following: children's safety and empowerment through school-based educational programmes and life skills, including comprehensive sex education;[167] providing parents, caregivers and educators with training and support; the implementation and enforcement of laws; community engagement and bystander intervention programmes; addressing "hotspots", structural drivers and inequalities; income and economic strengthening; and accessible child-friendly response and support services.[168]

88. It is therefore important that critical frontline and social services, including community-based systems, are strengthened to ensure that no child is left behind.[169] Significant research by the Centre of Expertise on Child Sexual Abuse exploring the availability of support services for children and adults affected by child sexual abuse revealed that waiting times for services have more than doubled since 2015, with an average of six months waiting time for much-needed support.[170] In total, 1 in 9 services have waiting lists that extend over a year. Furthermore, fewer services are dedicated to boys and men, persons with disabilities, people with ethnic minority backgrounds, faith groups and intra-familial or online abuse. Underresourced, understaffed and overburdened support services can cause further harm due to the significant delays and lack of comprehensive ongoing support. States must therefore invest in long-term, increased, sustainable funding of critical services to effectively attend to victims and survivors in a timely and sufficient manner.

89. According to the Committee on the Rights of the Child, the continued existence of these crimes contributes to a perception of the child as a sexual object and risks strengthening the belief among persons with a sexual interest in children that it is "normal" since many others share the same interest.[171] Addressing the root cause requires fostering early intervention programmes, effective counselling, therapeutic approaches, cognitive-behavioural theory methods, screening combined with interventions, and treatment programmes for at-risk and actual perpetrators, to

[164] See submissions from ECPAT Belgium, DEI, eSafety, European Centre for Law and Justice, Ordo Luris Institute and Dutch National Rapporteur Human Trafficking and Sexual Violence against Children.
[165] See A/HRC/56/48.
[166] See submissions from Colombia, Spain, NHRI Mexico and Partners for Transparency.
[167] WHO, *What Works to Prevent Online Violence against Children?* (Geneva, 2022).
[168] WHO, *INSPIRE Seven Strategies for Ending Violence against Children* (Geneva, 2016).
[169] See submission from UNICEF.
[170] Diana Parkinson and Milly Steele, *Support Matters: The Landscape of Child Sexual Abuse Support Services in England and Wales* (Barkingside, United Kingdom of Great Britain and Northern Ireland, Centre of Expertise on Child and Sexual Abuse, 2024).
[171] See CRC/C/156.

prevent them from acting on their desires and/or avoid recidivism, alongside working in conjunction with the criminal justice system.[172]

90. It should be noted that online deterrence campaigns and warning tools have reduced the total number of searches for child sexual abuse materials and direct users to prevention and therapeutic support services to change their problematic behaviour.[173] Approximately 74 per cent of users of the ReDirection Self-Help Program self-reported that they had reduced their use of or completely stopped viewing child sexual abuse material after starting the programme.[174]

91. Interventions for perpetrators of technology-facilitated child sexual abuse and exploitation remain limited, focused on adult male perpetrators (predominantly those known to the criminal justice system) with limited support provided for children, female perpetrators or the perpetrator's support network, such as family members or friends.[175] Insights should also be drawn into predatory behaviour analysis and human intelligence that examine the curators' intent when using technological products for their criminal activities.

92. Historically, adults were considered the most common perpetrators, but this now includes peer-to-peer violence.[176] Survey results of perpetrators on the dark web show that 70 per cent of perpetrators first saw child sexual abuse materials when they were under 18 years old, and nearly 40 per cent when they were under 13 years old.[177] Therefore, it is important to get a better understanding of and pay attention to this emerging concern to support children in (re)developing healthy sexual behaviours.[178]

VI. Conclusion and recommendations

93. **The existing and emerging harms caused through the misuse of technologies continue to grow as different types of platforms are being used for different purposes for the sale, sexual abuse and exploitation of children. Rapid technological development and change presents opportunities for organized criminal groups and perpetrators to adapt their modus operandi to target their victims. This raises the question about the effectiveness of current statutory and enforcement regimes, especially given the ease with which abuses and networks can be found in the digital environment.**

94. **Without immediate action, effective regulation, product safety and implementation of comprehensive public health approaches, this phenomenon will be further exacerbated by pre-existing inequalities, resulting in additional violations of the rights of children, with a disproportionate impact on those from vulnerable and marginalized groups.**

95. **Governments, law enforcement agencies and civil society continue to struggle to keep up with the rapid technological advancements and sophisticated criminal activities. If left unchecked, this can have long-lasting consequences, damage reputations and constitutes a permanent record of the abuse and violation of the dignity, privacy and sexual integrity of child victims and**

[172] See A/HRC/31/58.
[173] See submission from Lucy Faithful Foundation.
[174] Suojellaan Lapsia, "Feedback from users suggests that ReDirection Self-Help Programme successfully decreases CSAM use", 13 December 2022.
[175] Derek Perkins and others, *Interventions for Perpetrators of Online Child Sexual Exploitation: A Scoping Review and Gap Analysis* (Barkingside, United Kingdom of Great Britain, Centre of Expertise on Child Sexual Abuse, 2018).
[176] See submission from Lucy Faithful Foundation.
[177] See www.end-violence.org/safe-online.
[178] See submission from Dutch National Rapporteur.

survivors. It also increases the potential for re-victimization of known victims and survivors, as well as the victimization of children who were not initially victims of child sexual abuse and exploitation.

96. **A concerted effort from all stakeholders is required to respond to this problem, and technology companies have an important role to play in this regard. There is so much that can be done with the knowledge we already have. Children have the right to feel safe in all spaces, wherever they are. The Special Rapporteur as a result makes the recommendations below.**

97. **Regarding strengthening legal and policy frameworks, the Special Rapporteur recommends the following:**

(a) **Establish clear and comprehensive legislative frameworks with specific provisions that prohibit and criminalize all forms of sale, sexual exploitation and sexual abuse of children in the digital environment in accordance with international human rights standards;**

(b) **Ensure that national legislations do not criminalize child victims and survivors of the sale, sexual exploitation and sexual abuse;**

(c) **Impose strict criminal sanctions on industries and businesses that profit from technology-facilitated child sexual abuse and exploitation, including those that fail to assess and mitigate human right violations;**

(d) **Put in place comprehensive, child-centred and rights-based policy frameworks that specifically addresses technology-facilitated child sexual abuse and exploitation, and ensures the necessary technical support, capacity-building and coordination of activities across disciplines and sectors, including the public and private sector;**

(e) **Establish regular assessments and monitoring in order to systematically and adequately assess the impact of preventive interventions and strategies;**

(f) **Prioritize innovative, results-based prevention and public-health strategies that address structural and systemic inequalities, and will be accountable for reducing technology-facilitated child sexual abuse and exploitation over the short-, medium- and long-term.**

98. **Regarding regulation and oversight, the Special Rapporteur recommends the following:**

(a) **Establish and enhance the authority of competent national mechanisms or regulators to develop industry-specific codes and implement proper regulatory oversight of existing and emerging technologies, including of artificial intelligence models, virtual currencies, immersive technologies and end-to-end encryption technologies, to ensure appropriate child safety mechanisms are built in, in line with due process and the rule of law;**

(b) **Put in place measures to ensure that all technology companies introduce and abide by human rights safeguards, robust age verification and age-appropriate systems, child-friendly content moderation and pathways to referral and support services that adhere to the highest standards of ethics, placing privacy- and safety-by-design at the forefront of the engineering, development, deployment, operation and marketing of technological products and services to ensure that such applications or products do not facilitate or amplify the sale, sexual abuse and exploitation of children;**

(c) **Ensure that children's rights are mainstreamed within business models and value chains, including the implementation of meaningful child**

participation, safeguarding procedures, training of staff members and zero-tolerance approaches to any harmful and inappropriate behaviour towards a child;

(d) **Effectively put in place measures that ensure that technology companies invest, respect and sustain a focus on building their capacities to fulfil their responsibility to respect human rights across their activities, operations and business relationships, in line with the Guiding Principles on Business and Human Rights;**

(e) **Ensure that search engines and platforms that host applications and services regularly review and only accept applications that meet safety standards;**

(f) **Ensure that deterrence campaigns and warning tools in the digital environment are scaled across all platforms, directing users whose behaviour is problematic to prevention and therapeutic support services.**

99. **Regarding access to justice and support services, the Special Rapporteur recommends the following:**

(a) **Establish comprehensive and accessible reporting and referral systems for individuals, institutions, businesses, law enforcement authorities and the private sector, and ensure their use by fostering collaboration between the justice system and other key actors in the areas of child protection, education and health;**

(b) **Allocate sufficient and sustainable funding to make available and maintain referral and support services, including mechanisms such as 24-hour helplines to support and provide counselling services for both victims and survivors of sale, sexual abuse and exploitation, occurring both offline and in the digital environment;**

(c) **Ensure that reports are screened by trained professionals to ensure adequate and timely follow-up responses, and that emergency cases are responded to without undue delay to avoid putting the child in unnecessary peril;**

(d) **Ensure trusted flaggers and helplines are given the legal mandate to able to proactively search for and request the removal of content by flagging them to tech companies and online service providers;**

(e) **States that do not have facilities for hotlines or helplines are encouraged to partner with existing organizations to create an accessible national reporting mechanism, where citizens can report suspected child sexual abuse and exploitation in their own language;**

(f) **Finance urgent interim reparation measures for child victims and survivors of technology-facilitated sexual abuse and exploitation;**

(g) **Ensure that children who are required to participate in criminal justice proceedings are given age-appropriate, gender- and child-sensitive support and counselling to assist them at all stages of the proceedings;**

(h) **Remove procedural barriers that may cause and ensure safeguards against secondary victimization when victims and survivors seek recourse to justice, including statutes of limitations, that could prevent victims from coming forward, and provide easy access to child-sensitive complaint and reporting mechanisms;**

(i) **Provide trauma-informed therapeutic services and resources to promote healing for victims and survivors of technology-facilitated child sexual**

abuse and exploitation, including provisions for their care, recovery, rehabilitation and reintegration and for peer-to-peer support;

(j) **Ensure accessible and specialized mental health services for victims and survivors, fostering a culture of empathy and understanding that supports long-term sustainable arrangements to reduce the risk of re-traumatization;**

(k) **Establish and support the work of dedicated non-governmental organizations, advocates and activists, with a view to providing specialized support and services for victims and survivors;**

(l) **Foster early intervention programmes, effective counselling, therapeutic approaches and screening, combined with interventions and treatment programmes for potential and actual perpetrators.**

100. **Regarding research and cooperation, the Special Rapporteur recommends the following:**

(a) **Conduct research at the national level to provide comprehensive and evidence-based data to inform policies and strategies for safeguarding and responding to the needs of children who are victims and survivors of technology-facilitated sexual abuse and exploitation;**

(b) **Strengthen international cooperation, as required under the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, by sharing intelligence and exchanging information relating to the protection of victims and the apprehension of perpetrators, to support partnerships, cooperation frameworks and alliances among countries, international organizations and partners;**

(c) **Through a global multilateral mechanism dedicated to accelerating corporate responsibility actions and eradicating technology-facilitated child sexual abuse and exploitation, encourage the sharing of protocols, frameworks, practices, data analysis, expertise, classifications, reporting systems, technological equipment and processing capacities to foster international cooperation, while factoring the respective diversities, needs, circumstances and vulnerabilities of children in individual States and regions.**

101. **Regarding child participation, the Special Rapporteur recommends that the participation of children be encouraged in decision-making and technical standard-setting processes by involving and empowering them to share their ideas and knowledge about harmful behaviours and ways to report and prevent them, and that their proposals be taken into consideration, especially in the design, deployment and operation of technological products and services, as this will in turn increase the relevance and sustainability of these products and services.**

102. **Regarding knowledge-sharing, awareness-raising and capacity-building, the Special Rapporteur recommends the following:**

(a) **Promote mandatory digital literacy and school education programmes from early childhood onwards, on responsible online behaviour, mutual respect, healthy sexual relations, cybersecurity, privacy and safety, to enhance children's capacity to better protect themselves (and their peers) from harm and help them avoid and adequately react to risks that they may encounter online;**

(b) **Disseminate accessible child-friendly and gender-sensitive safety information, in the digital environment and offline, adapted to the child's age, maturity and local language, to inform them of the dangers of technology-**

facilitated child sexual abuse and exploitation, including reporting mechanisms, protection services and remedies available as a result of harms suffered;

(c) **Sufficiently equip, educate, train and support parents, caregivers, teachers and school counsellors to ensure a prompt and trauma-informed response to incidences of child sexual abuse and exploitation in the digital environment;**

(d) **Disseminate media campaigns using audiovisual materials that depict and reinforce norms and values relating to safeguarding children that go beyond home and school settings;**

(e) **Introduce awareness-raising on the sale, sexual abuse and exploitation of children into the syllabuses and learning materials of primary, secondary and higher learning institutions and schools;**

(f) **Provide training to strengthen the capacities of specialists, including social workers, psychiatrists, therapists, teachers, law enforcement personnel, lawyers and judges, respectively, to effectively identify, detect and investigate child sexual abuse and exploitation, rescue victims and prosecute and sanction offenders;**

(g) **Conduct training within the judicial sector on the harms suffered by child victims and survivors, including to their mental health and emotional well-being, so that they can better ensure that appropriate remedies, such as the provision of compensation, psychological support and rehabilitation, are made available to child victims and survivors.**