ECPAT'S SUBMISSION

Call for input: Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

15 May 2024

Introduction

This submission by ECPAT International[1] is in response to the call issued by the office of the Special Rapporteur on the sale and sexual exploitation of children to inform the forthcoming thematic report to the 79th session of the United Nations General Assembly in October 2024. This submission incorporates contributions made by several members of the ECPAT Network for the purpose of this call.[2]

How technologies are used to facilitate the sexual exploitation and abuse of children

When the Internet emerged into the public arena, law enforcement and hotline efforts focused largely on addressing the sharing of child sexual abuse material. However, as shared by multiple ECPAT members, subsequent developments in instant communications platforms, social media, and user-generated content platforms, as well as the advent of smart mobile devices and evolutions in AI and virtual environments, rapidly diversified the ways that children could be targeted online.

Underlying all child sexual abuse and exploitation are complex social dynamics that drive victimisation and perpetration, including by children and youth. However, recent trends include:

- **Scale:** Increase in child sexual abuse material and grooming taking place across multiple platforms
- **Complexity**:
    - Children are increasingly creating sexual content.
    - Live streaming of child sexual abuse leaves no digital trail.
    - Multi-platform exploitation has become more of the rule than the exception. Children are contacted on open platforms, such as messaging apps like TikTok, Snapchat or Kik, online games with chat functions (ECPAT Switzerland[3]) but also online marketplaces and classified ad websites (UYDEL in Uganda). They are then coerced to move to private, end-to-end encrypted platforms. ECPAT Korea also shares how offenders tend to target children who may appear more vulnerable, for example by searching on open platforms children who have used hashtags related to suicide or depression.

[1] ECPAT International is a global network of civil society organisations working to eradicate all forms of sexual exploitation of children. Over the past 30 years, ECPAT has become the forefront international NGO network dedicated to end this severe form of violence against children, advocating for State accountability and more robust measures across sectors to enhance the protection of victims. ECPAT currently has 126 member organizations operating in 106 countries around the world.

[2] ACRIDES, , Association Bayti, C-SEMA, Hope & Help, ECPAT Belgium, ECPAT Germany, ECPAT Indonesia, ECPAT Norway, ECPAT South Korea (Tacteen Naeil), ECPAT/STOP Japan, ECPAT Switzerland, ECPAT Taiwan, , FAPMI/ECPAT Spain, Uganda Youth Development Link (UYDEL), Women's Consortium of Nigeria.

[3] Caneppele S., Burkhardt C., Da Silva A., Jaccoud L., Muhly F., Ribeiro S. (2002). Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels. Available in French.

- Deepfakes and generative AI child sexual abuse material are rapidly becoming a severe challenge for child safety (FAPMI-ECPAT Spain and ECPAT Taiwan).
- AR/VR/XR and the Metaverse have the potential to expand the ways that children can be abused, with enhanced impact due to the onset of voice, touch, and other sensations.

- **Motivation:** New trends targeting children for financial gain, known as financial sexual extortion, are part of a re-emergence of commercialised or monetised forms of child sexual abuse, as distinct from primarily sexually motivated acts where the abusive images or contact with a child is the currency. In some countries, like Norway, boys are identified as primary victims of this type of crime.[4]

In addition to the above, digital technology has been increasingly used to facilitate traditional forms of child sexual exploitation and abuse. ECPAT members confirm that technology is increasingly playing a role in all forms of exploitation that they work to address. The Down to Zero Alliance, of which ECPAT is an implementing partner for global and regional advocacy, stresses that there is no clear boundary between in-person and online sexual of exploitation of children. As violations of sexual exploitation of children might occur online, in-person, or in varying geographies, it is vital that response mechanisms also use both online and in--person lenses. For example, in Belgium,[5] increase in the use of private rental platforms by intermediaries to rent out apartments that serve as meeting places for offenders and exploited children. This configuration makes detection by the authorities more difficult, as it is based on a system of instant bookings and confidentiality policies that limit collaboration with the authorities. Whether in the context of trafficking and migration, travel and tourism, in communities, or in online environments, it is no longer optional for child protection organisations to consider the technological dimensions of the issues they work to address. The way that technology interacts with existing forms of exploitation has both common and contextualised factors across regions and countries.

Practical recommendations for States, the technology industry and online service providers to prevent the sexual exploitation and abuse of children in the digital environment

Over the past decade or more, there have been significant advancements in law, policy, research, direct interventions and in the application of safety technology to prevent and respond to child sexual exploitation and abuse in digital environments. It is therefore important to acknowledge the existing global ecosystem of entities and professionals working in cooperation to address this shared challenge. However, substantial gaps remain in terms of action across sectors and geographies, and new challenges are constantly emerging that require coordinated action. As such, both States and the technology industry and online service providers have a duty to sustain and expand their respective responsibilities to act.

Practical Recommendations for States:

[4] Politiets Trusselvurdering. (2024). Kripos.
[5] ECPAT Belgium. (2023). Panorama de la situation des mineures victimes d'exploitation sexuelle en Fédération Wallonie-Bruxelles.

- Adopt future-proof, comprehensive and globally harmonised regulation that respects human rights and safeguards children's rights.
    - Hold companies accountable through legislative measures to invest in safety-by-design solutions.
    - Introduce mandatory risk assessment and transparency reporting based on harmonised standards.
- Enforce substantive legislation aimed at criminalising all forms of child sexual abuse and exploitation facilitated by technology, as well as procedural legislation on access to justice and legal remedies.
    - Make it compulsory, and subject to penalties, for Internet providers and website managers to block and/or report any material involving child sexual abuse proactively and without waiting for a request from the police.
    - Adopt and allow for more effective tools for virtual investigations by the police.
    - Introduce and enforce obligations on the financial sector to proactively detect and report suspected transactions involving child sexual abuse and exploitation.
- Collaborate around existing principles, standards, and approaches at global level.
- Collaborate between tech firms, government, and civil society to implement safety measures on digital platforms and develop advanced content detection and removal technologies.
- Invest in comprehensive prevention programmes:
    - Education in schools and communities remains crucial, as does fostering public awareness through public health and public safety messaging and mainstreaming of the topic in social debate, and professional training for frontline service providers and those working with children.
    - Media awareness about ethical reporting, terminology and nuanced, non-judgmental reporting of victimisation and perpetration.

Practical Recommendations for technology industry and online service providers:

- Develop and implement voluntary safety principles.
- Supplement legal compliance with risk-based safety measures that are built into existing and new products and features.
- Commit to innovation and collaboration within and between sectors:
    - Evolve detection tools to make use of innovative technologies to do so combined with human moderation.
    - Create easily accessible and transparent reporting mechanisms that inform users about the status of their report and measures that have been taken.
    - Develop, promote, and disseminate adequate technical measures such as Internet filters and child protection software.
    - Design age-appropriate products, including mandatory and accessible impact evaluations of their services. Adapt interfaces for children and implement pop-up warnings about online risks.
    - Make content child-friendly and understandable, especially about the implications of data collection and privacy conditions.
    - Include clear and age-appropriate warnings on products about safe and responsible use, targeting both children and families.

  - Develop age verification mechanisms that prioritise data protection and privacy.

- Engage in dialogue with governments, civil society, and the public about what works, what the challenges are, and what is and is not possible from a technical and/or legal perspective.

Gaps that limit the effective implementation and application of existing laws, policies and guidelines to prevent, detect, report and protect children from sexual exploitation and sexual abuse online

Civil society have observed an increase in cases of online or technology-facilitated child sexual exploitation in recent years, which has highlighted gaps to an effective response. ECPAT members highlight challenges associated with:

- Increasing power and resource imbalances that silence or marginalise civil society voices, a persistent lack of knowledge and awareness by the authorities, the media, tech platforms and civil society, as well as by children, families, and communities.
- Problems of definition and interpretation persist, creating ambiguity as to what constitutes online or technology-facilitated child sexual exploitation. This confusion is reflected in the lack of systematic recording of cases of sexual exploitation in institutional files, as well as in the failure to centralise data between the various sectors concerned.
- Despite significant recent years to research and measure the problem, for many countries there is still limited data on real cases, in part due to underreporting (resulting among others from lack of understand and awareness of risks associated with such crimes).
- Weak legislation and enforcement in the context of complex legal landscapes (including with regards to generative AI child sexual abuse material), with no or limited effective cross-sector collaboration and lack of a legal basis obliging platforms to systematically report and delete online child sexual abuse.
- Ethical and legal obstacles related to data sharing.
- Construed public debate that focuses solely on “chat control” which relates to end-to-end encrypted digital environments and supresses any discussion around other digital environments.
- Insufficient funding, resources, and qualified personnel to effectively tackle the problem, further complicated by problems of skills and information transfer, as well as a lack of collaboration with online platforms.

Existing challenges in the use of digital technologies, products or services, that inhibit the work of law enforcement across jurisdictions

- Cybercrimes are a transnational phenomenon and national regulation of platforms and service providers has only limited effect. Furthermore, the definition of the applicable jurisdiction can be complex.
- Law enforcement agencies lack sufficient funding and expertise in digital forensics, hindering effective action against online exploitation.

- Data protection and privacy laws combined with the implementation of end-to-end encryption on many communications platforms results in limited data sharing, wilful blindness to illegal activity, and obstacles to addressing the problem globally and at scale.
- Encryption technologies hinder law enforcement's ability to track offenders or access the information they need to investigate crime, complicating investigations and severely impacting child protection.
- The same technologies are among advanced tactics used by offenders to evade detection, making it difficult for law enforcement to combat their activities effectively.
- These challenges are both cause and consequence of the fact that communication platforms are not sufficiently regulated, e.g. often do not have appropriate safeguarding mechanisms and lack the obligation to report child sexual abuse material.

Technical and regulatory measures to be put in place by States, the technology industry and online service providers towards mitigating human rights risks associated of online child sexual exploitation and abuse

Robust, future proof and human-rights respecting legislation governing the digital environment is essential for society to tackle the challenge of online and technology-facilitated child sexual exploitation and abuse. At the same time, however, excessive fragmentation of legislative frameworks worldwide may create bottlenecks in building a sustainable cross-border response that includes harmonised legislation.

States that have so far failed to enact laws criminalising online and technology-facilitated child sexual exploitation and abuse must act to do so and harmonise measures with other jurisdictions. Specifically in the European Union, States must follow the recommendation relating to the European Commission Recommendation on developing and strengthening integrated child protection systems in the best interests of the child. It is essential that all the prevention and protection initiatives mentioned above are part of an integrated and child-centred child protection system.

States must also work together to share good practice and harmonise standards around key measures such as proactive detection, reporting and removal of child sexual abuse material online, and safety measures such as age verification and user authentication measures to prevent access to harmful content and enable the tracing of offenders. Such measures require regulatory bodies with a clear mandate to oversee compliance with laws and regulations.

Laws and oversight should extend to all areas of online service provision. For example, it is necessary to establish cooperation protocols aimed at facilitating detection and removal of content, between national authorities and rental platforms such as Airbnb and Booking.com, as well as social networks such as Snapchat, TikTok and Instagram.

The establishment and strengthening of reporting systems for users to flag illegal content, ensuring swift removal, is also essential. ECPAT Switzerland for example reports how the hotline Click and Stop allows for anonymous reporting of child sexual abuse material as well as providing professional, free

of charge and anonymous consultation for children, caregivers, professionals, and everyone who has a concern on online and technology-facilitated child sexual exploitation and abuse. Similarly, Tanzania has an established national helpline for reporting online or technology-facilitated child sexual exploitation which operates 24 hours and free of charge.

Practical examples of internal monitoring, complaint and reporting processes; establishment of regulatory bodies and interventions; remedial pathways; robust safeguarding procedures; children's rights' due diligence and risk assessments; and technical standard-setting processes to ensure safety and inclusivity by design

It is encouraging to report that there are numerous examples of legislation, policy and practice that are advancing collective action on child protection in the digital environment. Across the global ECPAT Network examples relate to **education, training and awareness raising, research, legal advocacy and multisectoral cooperation, as well as service delivery.**

In Africa, for example:

- In Namibia, Kenya and Malawi, ECPAT members are engaged in extensive advocacy, training and awareness raising, in particular highlighting gaps in parental awareness, in justice actors' training.
- In Cameroon, the ECPAT member works with technology companies to organise customised trainings for enhancing the use of the technologies to prevent abuse of use and exploitation of children.
- The ECPAT member in Burkina Faso specialised in child protection and have programmes including on child sexuality. They liaise with police and with the media to develop a response; the government has put in place measures but there are no specific measures for the online environment.
- In Nigeria, Namibia, Tanzania and Malawi, ECPAT members are engaged with national multi stakeholder initiatives including national taskforces.
- In The Gambia, civil society are advocating around the General Comment 25 on Children's Rights in relation to the Digital Environment.
- In Rwanda, there is ongoing work with journalists to train them on the topic.
- In Uganda, the existence of regional and national bodies like the Africa Civil Society Regional Network for UNTOC implementation (NET4U) Africa, Uganda Coalition against trafficking in persons, have been instrumental in building capacity of civil society on trafficking and topics related to online or technology-facilitated child sexual exploitation, and promoting anonymised reporting. In addition, there has been integration of children's rights assessments into the design and development of digital products and services.
- In Cap Vert there is now a national multisectoral network in place, as well as trainings on child rights and human rights ambassadors. The ECPAT member considers prevention on TV and radio with children and adults to be crucial.
- In Burkina Faso, the State has reviewed the law on communication and is working through a special police brigade and INTERPOL to identify perpetrators committing financial sexual extortion (known locally as *Bruteurs*), which is currently prominent in the media.

In the Middle East and North Africa region:

- In Morocco there have been advancement in law, but also the setting up of dedicated units to support women and children victims in violence, including online or technology-facilitated child sexual exploitation.
- The Disrupting Harm project - a multi-country research study on online child sexual exploitation and abuse led by ECPAT International, Interpol and UNICEF-Global Office of Research and Foresight – is ongoing in Morocco Tunisia and Jordan (as well as Armenia, Colombia, Dominican Republic, Mexico, Montenegro, North Macedonia and Pakistan).

Across Asia, examples include:

- Awareness and education programmes such as "Keep me safe" (Malaysia) and AMAN Warrior Program (Indonesia)
- Teacher trainings on identifying online or technology-facilitated child sexual exploitation and teaching online safety, training for social workers on how to support survivors and victims, and training for law enforcement on investigation.
- ECPAT members in many Asian countries, including Maldives, India and Nepal, members work with the travel and tourism sector to ensure that the fast-evolving role of technology in facilitating child sexual exploitation is acknowledged and acted upon.

From across Europe, examples include:

- The development in Austria of a handbook for professionals on how to handle child sexual abuse material and building an online platform for child safeguarding guidelines, including the digital dimension.
- In Spain, preventive work with families and children is taking place to support them to identify potential situations of risk, identify themselves as victims and learn about protection, and to inform specialized training for professionals and future professionals. In addition, recent legislative amendments have taken place better protect children in the digital environments.
- ECPAT Luxembourg conducts awareness in schools, including the development of tools (such as comics) targeted at youth.
- ECPAT Germany organised a conference on AI-generated child sexual abuse material that led to a short documentary on the topic. They are also exploring the links between online or technology-facilitated child sexual exploitation and human trafficking, and tourism. In Germany, a newly established monitoring standards for online service providers have been published by the BzKJ.

Across Central Asia, ECPAT members are working in research to inform advocacy and education. For example:

- CNZD Serbia has just initiated Project TUMAS aimed at establishing cooperation on online or technology-facilitated child sexual exploitation in the Western Balkans (Albanian, Serbia, North Macedonia) with goal of aligning legislation with the proposed EU Child Sexual Abuse Regulation.

- In Ukraine, despite the ongoing conflict, the ECPAT member is trying to address tech-facilitated as they are seeing new forms of sexual exploitation that they associate with children being mostly at home, with education being online, and with the lack of in-person communications channels. Social media are overwhelmed with intimate photos shared by children that can end up on more risky platforms. They have also observed an emergence and upsurge in adults trying to contact children for escort services, which did not previously target children. The response is to work closely with cybercrime colleagues and refer cases to law enforcement, and to support the process of amending the legislation to tackle this issue.

In Latin America, examples include:

- ECPAT México is cooperating with PACT-ECPAT USA and Hard Rock International on an app "*En busca de tu Identidad Virtual: Prevenir la Trata y la ESCNAA en línea''* that will be implemented in schools in popular travel and tourism regions.
- In Bolivia, they are producing guides to train computer science teachers about online or technology-facilitated child sexual exploitation.
- In Costa Rica, they have developed and led the *Código e-mentores,* an industry self-regulatory mechanism for online service providers to address tech-facilitated sexual exploitation and abuse of children.
- In Perú, they were instrumental in shaping Law 31664 that requires telecoms operators to inform their users about the use of parental filters to address online violence. They also operate an OSINT Cyber-Patrol to develop a glossary of terms to help identify potential perpetrators on social media and in online games.