



# Guiding principles for addressing technology-facilitated child sexual exploitation and abuse

Anri van der Spuy, Sabine Witting, Patrick Burton, Emma Day, Sonia Livingstone and Kim R. Sylwander

December 2024



# TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
Acknowledgements.....	5
<b>1. INTRODUCTION .....</b>	<b>6</b>
1.1. Aim and objectives .....	7
1.2. Target audience.....	7
1.3. Research methodology.....	9
1.4. Structure of the report .....	10
<b>2. CURRENT KNOWLEDGE .....</b>	<b>10</b>
2.1. Defining technology-facilitated CSEA in international law and policy.....	10
2.2. Evidence of technology-facilitated CSEA.....	15
2.3. Classifying forms of technology-facilitated CSEA.....	20
<b>3. INSIGHTS FROM EXPERT INTERVIEWS .....</b>	<b>24</b>
3.1 Conceptualising technology-facilitated CSEA .....	26
3.2 Understanding the role of technology in the context of violence, exploitation and abuse .	29
3.3 Understanding the position of the ‘child’ in technology-facilitated CSEA.....	36
<b>4. PRINCIPLES FOR ADDRESSING TECHNOLOGY-FACILITATED CSEA .....</b>	<b>40</b>
Principle 1: Children’s voices count .....	41
Principle 2: Language matters .....	42
Principle 3: Take care with context.....	44
Principle 4: Avoid blaming children .....	46
Principle 5: Future proof policy .....	48
Principle 6: Embrace a child rights approach.....	50
<b>5. CONCLUSION .....</b>	<b>52</b>
<b>6. REFERENCES .....</b>	<b>54</b>

# EXECUTIVE SUMMARY

This report addresses the pressing challenge of technology-facilitated child sexual exploitation and abuse (CSEA) by bridging the gap between the complexities of defining and classifying technology-facilitated CSEA and effective and appropriate responses and protection measures. Expert interviews, consultation and desk research reveal contrasting definitions and conceptions of technology-facilitated CSEA. These largely stem from the differences in terminology, context and the contrasting roles played by stakeholders, creating uncertainties and misunderstandings that impede effective responses.

Building on these insights and a statistical analysis of the Disrupting Harm evidence, the report sets out six principles by which diverse stakeholders can reach agreement in understanding and responding to technology-facilitated CSEA. These support policymakers, researchers, and practitioners with a holistic and context-sensitive child rights approach to addressing technology-facilitated CSEA and provide an entry point for professionals new to or with limited prior experience with the subject matter.

## **Principle 1: Children's voices count**

It is vital to take children's perspectives and experiences into account when making decisions, including the voices of child victims. Understanding how children perceive the dynamics of risks and harms in the digital environment is essential for developing effective interventions. This principle asserts that children's voices both enhance the credibility of the narratives concerning children's safety but also empower them.

## **Principle 2: Language matters**

Clear, consistent and precise terminology in policy, research and advocacy matters. Everyday terms used by children or the public are often at odds with those used in legislation or other formal contexts. Efforts are required to use language in ways that accurately reflect the experiences of children and the nature of the abuse. Without agreed language, we cannot reach a consensus on preventive and protective measures or societal recognition and endorsement of those measures.



## Acknowledgements

The Digital Futures for Children centre undertook this research as a contribution to the *Toolbox for Measuring Online Child Sexual Exploitation and Abuse* funded by the fourth Strategic Funding Call by the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) in turn funded by UK Research and Innovation (UKRI) as a three-year Centre of Research Excellence. This report benefited from significant input from stakeholders and partners, all of whom we thank for their time and expertise.

Expert interviews were conducted with Amy Crocker (ECPAT International), Iain Drennan (WeProtect), David Finkelhor (Crimes against Children Research Center, University of New Hampshire), Deborah Fry (University of Edinburgh and Childlight), Denton Howard (INHOPE), Sean Litton (Tech Coalition), Najat Maalla M'jid (UN Special Representative of the Secretary-General on Violence against Children), Helen Mason (Child Helpline International), Anastasia Shuster (Child Helpline International), and Michael Tunks (Internet Watch Foundation).

Online consultation participants included: Rangsimma Deesawade (Evident), Sakshi Ghai (University of Oxford, REPHRAIN research group), Shailey Hingorani (WeProtect Head of Policy, Advocacy and Research, core working group on the Luxembourg Guidelines), Daniel Kardefelt-Winther (Innocenti Global Office of Research and Foresight – UNICEF, REPHRAIN research group), Afrooz Kaviani Johnson (UNICEF), Simon Mason (independent law enforcement expert), Amy Orben (Programme Leader, University of Cambridge and REPHRAIN research group), Mama Fatima Singhateh (UN Special Rapporteur on the sale and sexual exploitation of children and sexual abuse of children), Ann Skelton (UNCRC Committee Chair, Professor University of Pretoria and Leiden University), James Stevenson (University of Edinburgh, core working group on the Luxembourg Guidelines), Serena Tommasino (Safe Online, Global Partnership to End Violence Against Children, core working group on the Luxembourg Guidelines), Naomi Trewinnard (Lanzarote Convention Secretariat, Council of Europe).

The report's independent peer reviewers: Hazel Bitaña (Child Rights Coalition Asia), Mariesa Nicholas (Australian e-Safety Commissioner's Office), Michael Salter (Childlight, University of New South Wales) and Fabio Senne (Brazilian Network Information Center, NIC.br). We also thank John Carr (Senior Expert Advisor on online child safety) and Beeban Kidron (Founder and Chair of 5Rights Foundation and the Digital Futures for Children centre).

# 1. INTRODUCTION

On the first day of 2024, it was reported that a 15-year-old girl in the UK had become what is believed to be the first known victim of rape in an immersive video game in the Metaverse.<sup>1</sup> Soon after, the Internet Watch Foundation<sup>2</sup> reported a significant and growing threat where Artificial Intelligence (AI) is used to produce child sexual abuse material (CSAM). Evidence of sexual risks and harms facilitated in one way or another by the use of technology and affecting children worldwide continues to mount, along with the need for practitioners to agree on how to define and understand these problems.<sup>3</sup>

The increasing acknowledgement of its impact on children, and indeed all victims, and its relationship to other forms of violence is reflected in how technology-facilitated CSEA is explicitly referred to in international treaties, instruments and policies, as well as national and regional commitments, policies and practices in different geographical and regional contexts. Significant initiatives exist at the regional level, such as the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse adopted by the Association of Southeast Asian Nations (ASEAN),<sup>4</sup> and the national level, such as the Tunisian National Plan of Action to End Online Violence Against Children<sup>5</sup> or the Kazakhstan 3 year action plan.<sup>6</sup> Spanning Global North and South countries, this reflects a global momentum to protect children from violence, including technology-facilitated CSEA.

While various important initiatives have contributed conceptual clarity regarding forms of technology-facilitated CSEA,<sup>7</sup> the pace of technological change and evolving online risks have pressurised shared understandings achieved thus far. This has consequences for how law and policymakers design and implement preventive and responsive measures and, consequently, how technology-facilitated CSEA is addressed more broadly. Hence, this report follows the United Nations (UN) Special Rapporteur on the sale, sexual exploitation and sexual abuse of children,<sup>8</sup> as well as the forthcoming revision of the Luxembourg Guidelines in referring to *technology-facilitated child sexual exploitation and abuse*. Avoiding technological determinism, this terminology highlights the role of human actors in using technology and that of businesses

---

<sup>1</sup> Sales (2024).

<sup>2</sup> IWF (2024b).

<sup>3</sup> ECPAT International (2022b, c, d); ECPAT International and UNICEF Office of Research – Innocenti (2022); INTERPOL (2023); UNICEF Office of Research – Innocenti (2022a, b); UNICEF Innocenti – Global Office of Research and Foresight (2023a, b); UNICEF Innocenti – Global Office of Research and Foresight & ECPAT International (2023).

<sup>4</sup> See [https://asean.org/wp-content/uploads/2021/11/4.-ASEAN-RPA-on-COEA\\_Final.pdf](https://asean.org/wp-content/uploads/2021/11/4.-ASEAN-RPA-on-COEA_Final.pdf)

<sup>5</sup> MFFES & UNICEF (2024).

<sup>6</sup> See Government of Kazakhstan (2023). In Kazakhstan, online protection, including the collection of nationally representative data, is included in the Comprehensive Plan on the Protection of Children from Violence, Suicide Prevention Ensuring their Rights and Well-being for 2023 to 2025.

<sup>7</sup> See, for example, ECPAT International (2016). An updated version of the Luxembourg Guidelines was finalised in October 2024.

<sup>8</sup> UNGA (2024).

in designing and deploying technology. It also highlights the significant continuities between CSEA online and offline.<sup>9</sup>

## 1.1. Aim and objectives

This report explores how key stakeholders navigate and understand the various definitions, measures and classifications of technology-facilitated CSEA before proposing a holistic child rights approach. The analysis critically unpacks the disagreements that experts face when addressing technology-facilitated CSEA and how these impact definitions, classifications and methodologies employed by researchers, policymakers, law enforcement and others.

We then propose principles for understanding and approaching technology-facilitated CSEA, which build on the considerable achievements of the last two decades in putting the topic of technology-facilitated CSEA on global and national political agendas. The principles also aim to complement existing and ongoing interventions to sharpen our understanding of and approaches to technology-facilitated CSEA in diverse contexts.

These principles seek to reconcile the complexities practitioners face through a holistic child rights approach based on the UN Convention on the Rights of the Child (UNCRC) and General comment No. 25 on children's rights in relation to the digital environment.<sup>10</sup>

## 1.2. Target audience

This report and the principles it develops are intended for researchers, policymakers and practitioners involved in identifying, preventing and responding to technology-facilitated CSEA. Since understanding technology-facilitated CSEA requires in-depth knowledge and understanding of child protection, digital technologies, and internet governance, we believe that the principles are a helpful entry point for understanding this critical challenge and relevant children's rights considerations. This may include audiences who are new to the topic, either because they have limited expertise in child protection or because they have limited expertise in the 'tech' aspect of technology-facilitated CSEA – such as helpline volunteers, early career researchers, government employees newly tasked with work in this field, and others. It may also include stakeholders with substantial expertise in specific domains since, as we show, what seems obvious to one expert may be unfamiliar to another. We seek to show how these differences in perspective may be resolved through a holistic children's rights approach.

---

<sup>9</sup> When we began this research, we used the term 'online child sexual exploitation and abuse' but found this term is poorly understood and contested insofar as 'online' does not adequately capture the range of contexts and dynamics that increasingly characterise individuals' experiences online or the wide range of devices and technologies through which CSEA can occur (ECPAT International, 2022a).

<sup>10</sup> 5Rights Foundation (2021); UN (2021).

## Toolbox for Measuring Online Child Sexual Exploitation and Abuse

This report contributes to this toolbox, funded by the UK National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN).<sup>11</sup> The aim was to examine differences, commonalities, gaps and barriers regarding the conceptualisation, classification and measurement of technology-facilitated CSEA in policy processes and large-scale surveys.

Led by Dr Amy Orben (University of Cambridge), the project leveraged two unique and comparable cross-national datasets that capture children's experiences of online risks: Disrupting Harm<sup>12</sup> and Global Kids Online.<sup>13</sup> It aimed to understand and measure technology-facilitated CSEA by elucidating the role of different risk factors in experiencing and reporting 'online child sexual exploitation and abuse',<sup>14</sup> advancing the conceptual understanding of online child sexual exploitation and abuse, and validating existing measurements in global populations to improve the future study of these harms.

**Work package 1** investigated how community (macro) and individual (micro) risk and protective factors predict the experience and disclosure of online sexual risks and harm by analysing the Disrupting Harm dataset developed by UNICEF Innocenti - Global Office of Research and Foresight, ECPAT and INTERPOL. It examined the demographic and country factors shaping children's experiences of a range of online sexual risks and harm across 27 countries. It provides a detailed statistical account of the distribution of nine specific measures of the incidence of these risks and harms reported by children.<sup>15</sup>

**Work package 2** examined the quality, validity and reliability of survey questions used in Disrupting Harm to capture different forms of technology-facilitated CSEA reporting measures across various countries and different child demographics. These investigations have enabled the development of an evaluation report of measures, the sharing of an analytical code for the analysis of measurement tools and a living best practice toolbox to measure technology-facilitated CSEA.<sup>16</sup>

**Work package 3** (*this report*) builds on the other work packages to develop a deliverable demonstrating best practice understanding of conceptualising, classifying and measuring technology-facilitated CSEA for research, policy and practice. It began with the idea of proposing an evidence-based classification of forms of child online sexual risks or harm. Informed by the analysis of Disrupting Harm and related surveys of children's online experiences and drawing on interviews with key policymakers concerned with addressing and combating technology-facilitated CSEA, this report develops six principles for researchers, policymakers and practitioners to guide future interventions.

<sup>11</sup> See [www.rephrain.ac.uk](http://www.rephrain.ac.uk)

<sup>12</sup> See <https://safeonline.global/disrupting-harm>

<sup>13</sup> See <http://globalkidsonline.net>

<sup>14</sup> The project's work packages 1 and 2 originally used the term 'online child sexual exploitation', reflecting usage in the Disrupting Harm project. This report, the outcome of work package 3, was specifically devoted to exploring the definitional differences represented in the field. Our present analysis led us to prefer 'technology-facilitated child sexual exploitation and abuse'.

<sup>15</sup> Ghai et al. (in preparation).

<sup>16</sup> Richards et al. (2024).



## 1.3. Research methodology

### Expert interviews

Expert interviews were the primary method to explore how key global experts understand, interpret and make meaning of technology-facilitated CSEA. We interviewed ten senior experts from global intergovernmental agencies, academic institutions, child helplines, organisations responsible for addressing risks associated with technology-facilitated CSEA and key practitioners working on related policy reforms in diverse contexts. Semi-structured individual interviews enabled participants to discuss the problem from their unique perspectives.<sup>17</sup>

### Analysis

We used thematic analysis to analyse perceptions of relevant practices in the interview transcripts. This helped to derive meaning from the cases by identifying and describing (implicit and explicit) ideas or themes 'in rich detail'.<sup>18</sup> Also, documentary sources were drawn on as needed and as referred to in the interviews. All this informed the development of the principles to bridge identified points of disagreement.

### Consultation to develop the principles

Informed by the project methods, we iteratively derived and discussed the principles during 2024. To complement our interviews, where most interviewees came from Global North contexts, an international high-level multistakeholder consultation was held on 30 July 2024, including stakeholders from both Global South and Global North contexts.<sup>19</sup> This aimed to:

- Benefit from a diverse range of views informed by different interests and stakeholder priorities and identify difficulties in addressing technology-facilitated CSEA.
- Gather input on the proposed principles' content, shape their wording, anticipate how they might be used by different stakeholders in diverse regions, and collect examples of each of the principles in action.

---

<sup>17</sup> Kvale & Brinkmann, 2008,

<sup>18</sup> Della Porta & Keating (2008, p. 31). The overarching themes in the topic guide were used to code each transcript using software (NVivo). We refined our codes by identifying patterns and consolidating or removing codes until we were satisfied that our codebook was telling useful stories relevant to our research problem. We identified three overarching themes, (i) current definitions; usefulness of definitions; related challenges; specific responses; (ii) dimensions of technology-facilitated CSEA, including abuse, violence and exploitation, the online/digital dimension and related challenges; (iii) actors implicated in technology-facilitated CSEA: the 'child'; the adult perpetrator; related challenges (including age of consent and determining intention).

<sup>19</sup> In total 15 experts (excluding the research team) participated in this consultation, representing different regions of the world including East Asia, Southern Africa, Europe and North America, the UK and several working across the globe. Participants were drawn from the child rights sector (including the Committee on the Rights of the Child and the Special Representative of the Secretary-General for the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography), violence against children and relevant researchers, law enforcement and child protection practitioners, as well as those involved in the 2024 revision of the Luxembourg Guidelines (see Acknowledgements).

## Ethics

The LSE Research Ethics Committee approved the project. The nature and purpose of the research were explained to participants when we reached out to request an interview. Before the agreed interview, we sent participants a consent form developed following LSE and REPHRAIN ethical guidance, which contained an information sheet about the intended research. Participants were asked to sign this form before or after the interview. When the interviews started, the project's purpose was reiterated to participants.<sup>20</sup> Before asking questions in the interview guides, participants could ask about the research and other ethical considerations. Regarding documents, we only relied on publicly available sources.

### 1.4. Structure of the report

In the next section (Section 2), we describe the landscape which frames current understandings of technology-facilitated CSEA. It considers how diverse actors and key documents describe difficulties in defining and understanding technology-facilitated CSEA and how these difficulties might translate to reporting and measuring technology-facilitated CSEA. Section 3 presents findings from interviews with key experts working on conceptualising, measuring and addressing technology-facilitated CSEA, followed by our proposed guiding principles for addressing technology-facilitated CSEA (Section 4). The report concludes in Section 5.

## 2. CURRENT KNOWLEDGE

### 2.1. Defining technology-facilitated CSEA in international law and policy

The scope of technology-facilitated CSEA varies considerably. Several key sources conceptualise the sexual abuse and exploitation of children within the broader international legal and policy landscape of children's rights.

- The ***United Nations Convention on the Rights of the Child (UNCRC)*** (1989),<sup>21</sup> in its Article 34, requires states to 'protect the child from all forms of sexual exploitation and sexual abuse', and it makes specific reference to preventing 'the exploitative use of children in pornographic performances and materials'. The UNCRC itself does not define the terms 'sexual abuse', 'sexual exploitation' or 'pornographic performance'.

---

<sup>20</sup> Allmark, et al. (2009).

<sup>21</sup> Bulger et al. (2017).

- A working group was established to develop an Optional Protocol to the UNCRC focusing on sexual exploitation and abuse,<sup>22</sup> resulting in the adoption of the ***Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC)*** (2000). The OPSC elaborates on different forms of sexual exploitation and abuse, defining the term ‘child pornography’ as ‘any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.’ It is important to note that the Committee on the Rights of the Child endorsed a terminology shift away from ‘child pornography’ towards terms such as ‘child sexual abuse material’, in one with conceptual developments among international actors.<sup>23</sup>
- In 2007, the ***Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse*** (CETS No. 201, also known as the Lanzarote Convention)<sup>24</sup> required the criminalisation of all kinds of sexual offences against children. It defines ‘child sexual abuse’ as sexual activities with a child who has not reached the legal age for sexual activities. Exploitation, in turn, is not explicitly defined in the Convention but is used in the context of various offences relating to ‘child prostitution’, ‘child pornography’ or ‘solicitation’ of children.
- In its 2019 *Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography*,<sup>25</sup> in addition to the criminalisation of ‘child pornography’, the Committee on the Rights of the Child drew attention to other forms of technology-facilitated CSEA that require dedicated attention in the context of the OPSC, such as grooming or sexual extortion. Here, we can see how the UN Committee on the Rights of the Child developed its understanding of concepts such as ‘child pornography’, ‘child sexual abuse material’ and child sexual exploitation as technology rapidly increased the ways that children can be abused and exploited.
- In 2021, the UN Committee on the Rights of the Child adopted ***General comment No. 25 on children’s rights in relation to the digital environment (CRC/C/GC/25)***<sup>26</sup> to guide relevant legislative, policy and other measures needed to ensure compliance with obligations under the UNCRC and its Optional Protocols concerning the digital environment. It contains multiple mentions of technology-facilitated CSEA-related risks

---

<sup>22</sup> Witting (2022).

<sup>23</sup> Committee on the Rights of the Child, *Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography*, CRC/C/156, para. 60. See also the Luxembourg Guidelines, 2016.

<sup>24</sup> See [www.coe.int/en/web/children/lanzarote-convention](http://www.coe.int/en/web/children/lanzarote-convention)

<sup>25</sup> Ibid.

<sup>26</sup> UN (2021). See also [www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation](http://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation)

and imposes associated obligations for Member States;<sup>27</sup> it does not explicitly define ‘sexual abuse’ or ‘sexual exploitation’ in the digital environment.

On a regional level, several organisations have incorporated definitions of child sexual exploitation and abuse in various conventions and other documents.

- The African ***Charter on the Rights and Welfare of the Child (ACRWC)*** requires states to take measures to prevent ‘the use of children in pornographic activities, performances and materials’ (Article 27). The definition is almost identical to Article 34 of the UNCRC. However, the ACRWC does not refer to the ‘use of children’ as ‘exploitative’. In its *General comment No. 7 on Article 27 of the ACRWC on sexual exploitation*,<sup>28</sup> the African Committee of Experts on the Rights and Welfare of the Child (ACERWC) defines child sexual exploitation and abuse as ‘any actual or attempted abuse of a position of authority, differential power or trust, for sexual purposes, including but not limited to profiting monetarily, socially or politically from the sexual exploitation of another’. Sexual exploitation of children can be commercial or non-commercial. It may include ‘exploitation of children in prostitution, the use of children in pornography, child trafficking for sexual exploitation and child marriage’. The General comment defines technology-facilitated child sexual exploitation as ‘all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment.’
- One of the most influential global efforts at harmonising terms and definitions related to child protection is the ***Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*** (known as the Luxembourg Guidelines),<sup>29</sup> an initiative by 18 international partners and led by **ECPAT International**.<sup>30</sup> The Guidelines aim to facilitate agreement among a multitude of actors (such as UN entities, international child rights non-governmental organisations (NGOs) and international and regional law enforcement agencies) regarding what terms to use to describe different forms of sexual exploitation and sexual abuse of children. They define ‘online child sexual abuse’ as ‘any form of sexual abuse of children ... which has a link to the online environment’ and ‘online child sexual exploitation’ as ‘the use of the internet as a means to exploit children sexually’. The forthcoming second edition of the Luxembourg Guidelines regards the term as having ‘a generally agreed meaning’. Note that ‘special attention should be paid’ when using the term ‘online child sexual abuse.’ The guidelines will refer to technology-facilitated CSEA as the preferred terminology in the forthcoming edition. This terminological shift away from ‘online child sexual exploitation and abuse’

---

<sup>27</sup> See, for example, paras 2, 25, 71 and 81.

<sup>28</sup> ACERWC, *General Comment No. 7 on Article 27 of the ACRWC* (2021).

<sup>29</sup> ECPAT International et al. (2017).

<sup>30</sup> ECPAT International (2016).

denotes how the term 'online' fails to capture the full breadth of ways through which technologies facilitate child sexual exploitation and abuse.

- The **Tech Coalition**, a membership-based organisation for technology companies that focuses on various activities to 'protect children online',<sup>31</sup> uses the term 'online child sexual exploitation and abuse', which is defined as 'the usage of the internet or communication technologies to facilitate the sexual abuse of children and adolescents.' It does not, therefore, mention 'exploitation' in its definition. It provides examples of online child sexual exploitation and abuse, namely 'grooming, sexual extortion, sexting, live streaming, perceived first-person (often called "self-generated"), and child sexual abuse materials (CSAM)'. In respect of the latter, it further elaborates that although 'there is no single legal definition for online CSAM, this term – which is still legally known as child pornography in the USA – generally refers to sexually explicit imagery involving a child.'
- The **WeProtect Global Alliance**<sup>32</sup> is a global and multistakeholder alliance of actors addressing technology-facilitated CSEA, including governments, private sector companies, civil society organisations and intergovernmental organisations. In its annual *Global Threat Assessment report*,<sup>33</sup> it defines 'child sexual exploitation and abuse online' as 'child sexual [exploitation and] abuse that is partly or entirely facilitated by technology, i.e. the internet or other wireless communications'. It situates CSEA slightly differently than other organisations within the context of digital environments, explaining: 'We use the term child sexual exploitation and abuse online, or "internet-enabled abuse", and not online child sexual exploitation and abuse to avoid characterising abuse online as distinct from abuse offline, since for victims the abuse is often not confined to the online realm.'<sup>34</sup> Over 40 countries have implemented WeProtect's Model National Response (MNR), which guides multi-stakeholder country responses to technology-facilitated CSEA encompassing six elements: legislation and policy frameworks; prevention strategies; law enforcement training; collaboration with the private sector; data collection and research; and victim support services.<sup>35</sup> The MNR thereby outlines the infrastructure needed for effective protection and response.

---

<sup>31</sup> See [www.technologycoalition.org/the-issue](http://www.technologycoalition.org/the-issue)

<sup>32</sup> See [www.weprotect.org](http://www.weprotect.org)

<sup>33</sup> WeProtect Global Alliance (2023).

<sup>34</sup> Ibid.

<sup>35</sup> <https://www.weprotect.org/framing-the-future/>

## **General comment No. 25 includes the following on technology-facilitated CSEA**

### **On violence, exploitation and abuse**

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

States parties should take legislative and administrative measures to protect children from violence in the digital environment, including the regular review, updating and enforcement of robust legislative, regulatory and institutional frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment. (para. 82)

### **On the role of the business sector**

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

### **On children's rights to privacy**

Privacy is vital to children's agency, dignity and safety and for the exercise of their rights. (para. 67)

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

### **On children's right to freedom of expression**

Content controls, school filtering systems and other safety-oriented technologies should not be used to restrict children's access to information in the digital environment; they should be used only to prevent the flow of harmful material to children. Content moderation and content controls should be balanced with the right to protection against violations of children's other rights, notably their rights to freedom of expression and privacy. (para. 56)

Any restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate. The rationale for such restrictions should be transparent and communicated to children in age-appropriate language. (para. 59)

## 2.2. Evidence of technology-facilitated CSEA

Society's ability to report, detect and monitor these risks is improving.<sup>36</sup> However, sustaining a global evidence base for technology-facilitated CSEA remains challenging, given differences in language, conceptualisation, measurement and reporting, as well as ethical, definitional, cultural and sociopolitical concerns.<sup>37</sup>

### Insights from reports to helplines and related statistics

Reporting statistics, whether to CSAM hotlines or child helplines, and national crime statistics, provide essential indications of reporting trends. The Internet Watch Foundation (IWF) reports that they received and assessed 392,665 reports of suspected CSAM in 2023, while 275,652 URLs were confirmed to contain CSAM.<sup>38</sup> The IWF defines the term CSAM term as 'images or videos that show the sexual abuse of children' without further explaining which actions the term 'sexual abuse of children' includes.

The National Center for Missing & Exploited Children (NCMEC), a US-based child protection organisation, reports that in the same period, their CyberTipline fielded 36.2 million calls relating to suspected technology-facilitated CSEA, of which 99 per cent were related to suspected CSAM.<sup>39</sup> NCMEC defines the term 'sexual exploitation' broadly, stating that sexual exploitation of children includes 'nudes or sexual images/videos of a child; someone chatting online with a child about sex; sexual abuse of a child that occurs offline; someone seeking or offering a child for sexual acts in exchange for something of value (e.g., money, food, gas, shelter, clothing, drugs); unwanted sexual emails or texts either involving children or sent to a child; websites or domains that contain sexual content but have similar names or URLs to mainstream sites that may be misleading to children; websites or domains that have sexual content (words or images) embedded in them which minors might see.'

Child Helpline International,<sup>40</sup> an organisation with over 150 child helpline members in more than 130 countries, defines the term 'online sexual exploitation and abuse' as 'all acts of a sexually exploitative nature carried out against a child that is at some stage connected to the online environment'.<sup>41</sup> The term is explicitly distinguished from 'online child sexual abuse' in that it contains 'an underlying notion of exchange, for example, money, food, accommodation, drugs, affection, gifts, etc.' It defines child sexual abuse separately as 'the involvement of a child in sexual activity that they do not fully comprehend, that they are unable to give consent to, that they are not developmentally prepared for and/or is in violation of law.'

---

<sup>36</sup> ECPAT International (2020a).

<sup>37</sup> See, for example, Child Helpline International (2023); Finkelhor et al. (2023a); Ghai et al. (2022); Martin et al. (2023); UNGA (2023a); UNICEF Office of Research – Innocenti (2022b); WHO (2022).

<sup>38</sup> IWF (2024a).

<sup>39</sup> See NCMEC's reporting statistics here: <https://www.missingkids.org/cybertiplinedata>

<sup>40</sup> See <https://childhelplineinternational.org>

<sup>41</sup> Child Helpline International (2023).

All these sources provide valuable insights into the scale of technology-facilitated CSEA. However, the different definitions and measures employed to measure and define such reports vary significantly.<sup>42</sup> These differences impede the assessment of the prevalence and classifications of forms of technology-facilitated CSEA. Changes over time (trends) may be indicative of public recognition of the harms or awareness of reporting systems or mechanisms and take-up of those mechanisms rather than an accurate depiction of the actual prevalence.<sup>43</sup>

However, national crime statistics usually grossly underrepresent actual prevalence as they show the cases that reach the criminal justice system based on national definitions of criminal behaviour, which may not align with internationally recognised forms of exploitation and abuse.<sup>44</sup> Further, national definitions and provisions of criminal behaviour often fail to encompass technology-facilitated CSEA cases that have an online and offline element, and such cases might be solely recorded as a contact offence (e.g., rape), thereby neglecting the online component. In short, there are difficulties in capturing the full extent of technology-facilitated forms of exploitation and abuse in criminal justice statistics, particularly in countries that have yet to develop the necessary dedicated criminal provisions.<sup>45</sup>

## Qualitative research insights into the views and experiences of victims

Research with adults and children who have experienced technology-facilitated forms of CSEA provides essential insight into their framing of these experiences. Qualitative studies that illustrate the contexts and circumstances of children's experiences and strategies related to incidents of exploitation and abuse are important in identifying children's priorities for action while also exemplifying the complexities of these issues.<sup>46</sup> An interview study with 33 young people in five different countries conducted as part of the Disrupting Harm project illustrates how the risks young people face when online are shaped by their specific socioeconomic, cultural and individual circumstances—including previous experiences of violence, abuse and other vulnerabilities.<sup>47</sup> The same study shows how experiences of exploitation and abuse can sometimes be complexly entangled with enjoyable, exciting and positive exchanges online until they are not, and the situation becomes abusive.

A recent qualitative study with 604 children from seven countries,<sup>48</sup> including high-, middle- and low-income settings, illustrates children's experiences of online grooming in their everyday

---

<sup>42</sup> For example, NCMEC includes websites depicting sexual content in its definition of sexual exploitation of children, which does not fall under the narrower definitions established by Child Helpline International. In addition, the IWF does not include an element of 'exploitation' in its definition of 'child sexual abuse imagery', whereas Child Helpline International provide separate definitions of exploitation and abuse.

<sup>43</sup> Conversely, declining reports made over time may be a reflection of the actual prevalence, or could be reflecting a lack of trust or faith in the system or declining awareness of the mechanism. In short, while data from hotlines or helplines might provide *some* indication of technology-facilitated CSEA in society, they cannot be deemed reliable or accurate depictions of the status quo.

<sup>44</sup> INTERPOL (2023).

<sup>45</sup> Ibid.

<sup>46</sup> ECPAT International (2022a).

<sup>47</sup> ECPAT International (2022a).

<sup>48</sup> Third et al. (2024).



digital activities. The study illustrates how children navigate these risks and identifies ways that protections can be developed and improved based on children's actual use of various platforms in different countries, including their strategies to mitigate risks. This study, like other research, including from the Disrupting Harm project, shows that children more often experience abuse by people they know rather than unknown people on the internet.<sup>49</sup> They noted cultural differences between the countries, for instance, in how they define strangers online and respond to encounters with unknown people online. Delving into children's lived experiences identifies the need for sensitive approaches that consider children's ways of navigating and understanding the risks and harms they are exposed to online and beyond.

### **Acknowledging victims' voices**

**Canadian Centre for Child Protection:** This study documents the lived experiences of 281 victims of CSAM, illustrating the difficulties victims face when reporting these instances to service providers and the consequences of companies' inaction. These detailed victim testimonies provide actionable insights to reduce harm to children online, as they describe the technologies that facilitate the abuse they have faced, as well as the consequences of companies' inaction:

'You can't delete or remove videos on the internet once they're there, someone is always going to have a copy... It has always felt like I can do nothing about it and I doubt anything would come out of it. You can request removal but at least one paedophile has probably saved it.'<sup>50</sup>

'I have [reported child sexual abuse material] a few times off YouTube. ABSOLUTELY NO RESPONSE.'<sup>51</sup>

'It's a slap in the face having companies cite user privacy when refusing to take down the material. You'd think that child sexual abuse material would be an exception to privacy laws, but I guess not.'<sup>52</sup>

**Disrupting harm:** The experiences victims share show how technology-facilitated CSEA tends to be intertwined with in-person abuse throughout a continuum of abuse. Their stories reveal their contexts of vulnerability to technology-facilitated CSEA and where efforts and support are needed:

'No, I did not [tell my mother] because I was afraid because my mom had warned me not to communicate with people that I do not know on social media, so I was afraid that she will criticise me for doing that. I had to be my own rock, ma'am.'<sup>53</sup>

<sup>49</sup> UNICEF Innocenti – Global Office of Research and Foresight (2023b).

<sup>50</sup> Canadian Centre for Child Protection (2024, p. 9).

<sup>51</sup> Ibid, p 13.

<sup>52</sup> Ibid.

<sup>53</sup> ECPAT International (2022a, p. 22).

## Quantitative insights from representative survey research

The available evidence of the incidence, nature and scale of technology-facilitated CSEA indicates that the problem is worsening.<sup>54</sup> Specifically, there have been improvements in survey methods with children to understand their experiences of technology-facilitated CSEA, most notably through the Disrupting Harm project.<sup>55</sup> Tech companies have also developed monitoring and research on the prevalence of CSEA on their platforms, although these are seldom made public.<sup>56</sup>

Recent reports indicate that hundreds of millions of children have experienced some form of technology-facilitated CSEA in the past year. A recent meta-analysis of 125 studies conducted in 57 countries estimated that 1 in 8 children globally have been subjected to online solicitation in the past 12 months, and 1 in 8 have also experienced non-consensual taking, sharing or exposure to sexual images.<sup>57</sup>

Different measurement methods (e.g., counting offences, perpetrators, victims/survivors or materials)<sup>58</sup> result in varying prevalence estimates across research teams and countries. Some research continues to conflate risk and harm<sup>59</sup> in measuring technology-facilitated CSEA, undermining the accuracy of estimates made.<sup>60</sup> Cultural differences and cultural stigma regarding sexual exploitation and abuse also influence respondents' answers to survey questions. Too often, individual measures are insufficiently grounded within the relevant contextual and cultural values and understanding of language and terminology across geographies. This may be as simple as the interpretation of 'sexual pictures', which may assume different meanings in different contexts, ranging from depictions of genitalia or sexual activity in one context to lingerie adverts in others.<sup>61</sup> The assumptions based on those simple measures may thus be undermined by a lack of the contextual information required to fully understand the experience and the potential or likelihood for harm to result from that experience.

Disrupting Harm is a research project conducted as a partnership between UNICEF Innocenti—Global Office of Research and Foresight with ECPAT International and INTERPOL, funded by the Safe Online Initiative and building in part on measures developed by Global Kids Online.<sup>62</sup> Its survey questionnaire has proposed a solution to the above methodological challenges by

<sup>54</sup> See, for example, Colburn et al. (2023); Finkelhor et al. (2023a).

<sup>55</sup> See UNICEF Office of Research – Innocenti (2022b). Read more about the Disrupting Harm research project at <https://safeonline.global/disrupting-harm>

<sup>56</sup> A part of the increase in known cases may result from increased active detection of technology-facilitated CSEA and improved reporting mechanisms. This is partly due to more stringent regulations that require companies to publish transparency reports or to undertake child rights due diligence or otherwise incentivise companies to detect and report harm proactively. On the other hand, recent technological developments have also increased the ease by which CSEA can be spread through encrypted channels.

<sup>57</sup> Childlight (2024).

<sup>58</sup> Quayle (2021).

<sup>59</sup> Livingstone (2013).

<sup>60</sup> Stoilova, Livingstone & Khazbak (2021).

<sup>61</sup> See, for example, UNICEF East Asia and Pacific & Centre for Justice and Crime Prevention (2020).

<sup>62</sup> Stoilova, Livingstone & Kardefelt-Winther (2016).

including in its measurement of technology-facilitated CSEA a set of questions that could be asked directly of children and that are designed to capture behaviours that appear, at face value, clearly harmful to a child, and that in most jurisdictions would be considered illegal. The survey items were also designed in a way that recognises that sexual risks do not inherently equal sexual harm but will vary, and the degree of harm caused will depend on the child’s life circumstances. The result is the most sizable, robust and comparable dataset relating to children’s experiences of technology-facilitated CSEA.

The Disrupting Harm dataset currently includes 12 countries – and 11,912 children<sup>63</sup> (in Eastern and Southern Africa and Southeast Asia).<sup>64</sup> UNICEF Innocenti—Global Office of Research and Foresight conducted nationally representative household surveys to collect data from 1,000 children aged 12 to 17 and 1,000 caretakers per country. The research examined children’s exposure to each of nine key measures of online sexual risks and harms, as shown in Table 1.

Table 1: Nine Disrupting Harm measures

<p><b>a) Unwanted sexual comments</b></p> <p>“Someone made sexual comments about me (e.g. jokes, stories or comments about my body, appearance or sexual activities) that made me feel uncomfortable.”</p>	<p><b>e) Solicited sexual images/videos</b></p> <p>“I have been asked for a photo or video showing my private parts when I did not want to.”</p>
<p><b>b) Unwanted sexual images</b></p> <p>“Someone sent me sexual images I did not want.”</p>	<p><b>f) Commercial images/videos</b></p> <p>“Someone offered me money or gifts in return for sexual images or videos.”</p>
<p><b>c) Unwanted sexual talk</b></p> <p>“I have been asked to talk about sex or sexual acts with someone when I did not want to.”</p>	<p><b>g) Non-consensual image sharing</b></p> <p>“Someone shared sexual images of me without my consent.”</p>
<p><b>d) Unwanted sexual act requests</b></p> <p>“I have been asked by someone to do something sexual when I did not want to.”</p>	<p><b>h) Commercial sexual act requests</b></p> <p>“Someone offered me money or gifts to meet them in person to do something sexual.”</p>
	<p><b>i) Sexual extortion</b></p> <p>“Someone threatened or blackmailed me to engage in sexual activities.”</p>

<sup>63</sup> ECPAT International (2022a, b, c, d); ECPAT International and UNICEF Office of Research – Innocenti (2022); INTERPOL (2023); UNICEF Office of Research – Innocenti (2022a, b); UNICEF Innocenti – Global Office of Research and Foresight (2023a, b); UNICEF Innocenti – Global Office of Research and Foresight & ECPAT International (2023).

<sup>64</sup> Data collection for another 11 countries (in the Middle East and North Africa, Eastern Europe, Latin America and South Asia) is underway for 2024/5.

It also examined the likelihood of children disclosing such experiences to the police, helplines, a friend, parent, guardian or other responsible adult, together with the patterning of these results by different demographic and sociocultural factors.

The first two work packages of the *Toolbox for Measuring Online Child Sexual Exploitation and Abuse* project (of which this report is the third work package) analysed the data generated by these nine survey questions to identify the robustness of the measures and determine whether the findings could predict children's experience and reporting of online sexual risks and harms.

Work package 1<sup>65</sup> analysed individual demographics (age, gender) and country correlates of the measures used in the Disrupting Harm surveys in these 12 countries. The findings show that up to 20 per cent of children who use the internet in these countries said 'yes' to at least one of measures f, g, h or i.<sup>66</sup> When examining any or all of the nine measures, Ghai and colleagues found a weighted estimate of 17 per cent, one out of six children self-reporting experiencing any of these measures (from a to i).<sup>67</sup> Further, older children were more likely to report such experiences than younger children, but there was no statistical difference by gender.<sup>68</sup>

## 2.3. Classifying forms of technology-facilitated CSEA

There is considerable divergence in the conceptualisation and measurement of technology-facilitated CSEA, yet the need for terminological clarity is widely acknowledged. The UN's World Health Organization (WHO), for instance, warns that definitional and conceptual discrepancies may not only 'confuse stakeholders about where to look or what goals and topics are being addressed by various programmes' but 'is a clear impediment to progress, the accumulation of knowledge, and programme development, adoption, and dissemination'.<sup>69</sup> Similarly, UNICEF acknowledges the difficulty in measuring the prevalence and nature of violence against children since there is no agreed operational definition at the international level.<sup>70</sup> Without agreement and alignment on how technology-facilitated CSEA and related risks might be understood, identified or defined, it can be difficult to appropriately and responsibly deal with or manage associated risks related to technology-facilitated CSEA.

---

<sup>65</sup> Ghai et al. (in preparation).

<sup>66</sup> ECPAT International (2022b, c, d); ECPAT International and UNICEF Office of Research – Innocenti (2022); INTERPOL (2023); UNICEF Office of Research – Innocenti (2022a, b); UNICEF Innocenti – Global Office of Research and Foresight (2023a, b); UNICEF Innocenti – Global Office of Research and Foresight & ECPAT International (2023). For results from each country, see <https://safeonline.global/disrupting-harm>

<sup>67</sup> Ghai et al. (in preparation).

<sup>68</sup> When looking at the interaction between age and gender, older girls reported slightly more risks compared with boys. When looking at country differences, the rates of online sexual risks and harms varied between countries, ranging from an estimated 0.3 per cent of digitally connected children in Vietnam to 29 per cent in the Philippines. As noted elsewhere, caution is needed, given that cultural factors may result in under-reporting in certain countries (Ghai et al., in preparation).

<sup>69</sup> WHO (2022).

<sup>70</sup> UNICEF (2023).

Against this background, several interventions have been undertaken to address this issue. As mentioned, one of the critical interventions on terminology around child sexual exploitation and abuse is the so-called *Luxembourg Guidelines*. Initially published in 2016, the Guidelines aim to provide ‘universal’ language for terms commonly used in the context of sexual exploitation and sexual abuse of children. They review the meaning of each term from a linguistic point of view and recommend which terms should be avoided or where there is a need for caution in using a particular term. The guidelines are under review and will likely be published towards the end of 2024.

Further, in 2023, UNICEF developed an International Classification of Violence Against Children (ICVAC). This aims to address the divergent operational definitions and concepts around violence against children, including technology-facilitated CSEA. Typical incidents of technology-facilitated CSEA against children, such as grooming, live-streaming of sexual abuse or non-consensual image-taking of the sexual organs of or sexual activities with a child, are used as illustrative examples under the category of ‘non-contact sexual violence against children’. However, the ICVAC acknowledges that violence can take place simultaneously in multiple settings, in particular, if technology is involved, and recommends that in such cases, the relevant settings should be tagged to the specific act of violence. The ICVAC is, therefore, a helpful instrument in classifying different acts of violence against children, including technology-facilitated CSEA, in the context of statistical data.

Another key intervention is the EU Kids Online’s 4Cs categorisation of online risks,<sup>71</sup> which has become an important reference point in the field. The 4Cs informed much of the thinking reflected in the approaches to sexual risks and harms and terms adopted by the organisations just mentioned. Developed from the EU Kids and Global Kids online datasets, the 4Cs do not attempt to create a new classification of technology-facilitated CSEA. Instead, ‘sexual’ is part of the vertical axis (distinguished from aggressive and value-based risks) in a table that maps risks horizontally according to content, contact, conduct and contract (the 4Cs, See Table 2).

This approach recognises that risks arise when a child engages with or is exposed to potentially harmful content or experiences or is targeted by potentially harmful contact; witnesses, participates in or is a victim of potentially harmful conduct; or is a party to or exploited by a potentially harmful contract. The 4Cs classification also distinguishes between aggressive, sexual and value risks and recognises cross-cutting risks to children’s privacy, health and fair treatment. Among other things, the 4Cs model is a helpful starting point for understanding a range of risks related to technology-facilitated CSEA and recognising that risks are always relational: they result from the dynamic interaction between the child’s agency and those operating in the digital environment.

---

<sup>71</sup> Livingstone & Stoilova (2021); Stoilova, Rahali & Livingstone (2023).

One of the problems with developing classifications and typologies in research, for instance, is that they are only effective when all are in agreement, as their inconsistent application will skew results across geographies. Classifications are also linked to varied understandings and qualifications of which actions are considered risks or harms. These difficulties of classification are evident in Childlight’s meta-analysis of 125 studies in 57 countries, where they propose different types of technology-facilitated CSEA to reach some level of uniformity in their analysis: online solicitation; non-consensual taking, sharing and exposure to sexual images and videos; online sexual exploitation (commercial sexual talk, commercial sexual images or other commercial sexual activity and sexual coercion); and sexual extortion (making a threat to disseminate sexual images to obtain money, additional pictures or other sexual activities).<sup>72</sup>

Table 2: The 4Cs

 CORE	<b>Content</b> Child as recipient	<b>Contact</b> Child as participant	<b>Conduct</b> Child as actor	<b>Contract</b> Child as consumer
<b>Aggressive</b>	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
<b>Sexual</b>	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
<b>Values</b>	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
<b>Cross-cutting</b>	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Source: <https://core-evidence.eu/posts/4-cs-of-online-risk>

However, few of the studies reported on more than one type of violence, and fewer included multiple measures, lowering the validity of overall prevalence measures and making comparisons difficult. The results show high variability across studies, from 1 to 37 per cent for lifetime and 3 to 34 per cent for the past year. Emerging forms of technology-facilitated CSEA also challenge stable and uniform typologies. This broad variability in prevalence findings indicates varying methodologies and the lack of studies that include a broader range of technology-facilitated CSEA types across the literature. The report concludes that this highlights the need for more accurate measurements and categorisation of victimisation experiences.<sup>73</sup>

<sup>72</sup> Childlight (2024).

<sup>73</sup> Ibid, p. 18.

## Disrupting Harm findings about the forms of technology-facilitated CSEA

The second two work packages of the *Toolbox for Measuring Online Child Sexual Exploitation and Abuse* project explored possible clusters or types of online sexual risks or harms based on the correlations observed among the nine measures in the Disrupting Harm dataset shown in Table 1. Richards and colleagues show that all nine measures were moderately or strongly intercorrelated.<sup>74</sup> This confirms the widespread finding in the literature of poly-victimisation (or co-morbidity): children who encounter one risk or harm are more likely to experience others as well.<sup>75</sup> Forthcoming analysis using the Disrupting Harm dataset has further demonstrated that children who experience multiple online risks and harms report higher rates of anxiety, suicidal thoughts or behaviours and acts of self-harm.<sup>76</sup>

While this research only examined measures related to technology-facilitated sexual risks or harms, other research shows that poly-victimisation also encompasses non-sexual risks (e.g., a child who has seen online hate or violence is more likely to encounter sexual risks).<sup>77</sup> Such research links offline and online risks, most often interpreted as showing that children at risk in their offline lives are more likely to be at risk online. Research has also shown that most children who experience online sexual violence have also experienced in-person sexual violence.<sup>78</sup>

The research also evaluated the quality, validity and reliability of the nine items related to technology-facilitated CSEA in the Disrupting Harm dataset.<sup>79</sup> Exploratory factor analysis identified a reliable, well-fitting two-factor structure validated through confirmatory factor analysis (see Table 1). Given the challenges in quantifying harms in population surveys, these factors were labelled as 'risk of sexual exploitation' (four items) and 'risk of sexual harassment and abuse' (five items). This structure aligns with the distinction policymakers often make between exploitation and abuse (see Table 3).<sup>80</sup>

Richards and colleagues also found weaker evidence for a three-factor structure that distinguishes measures a and b (potentially labelled 'risk of sexual harassment') from c, d and e (potentially labelled 'risk of sexual abuse').<sup>81</sup> Although a further two-item factor (potentially labelled 'risk of sexual harassment') showed insufficient reliability, future items could be developed, resulting in a stronger scale with good construct validity.

<sup>74</sup> Richards et al. (2024).

<sup>75</sup> See also Finkelhor et al. (2007); Finkelhor et al. (2024 a; b).

<sup>76</sup> Kardefelt-Winther et al. (2025).

<sup>77</sup> WHO (2022).

<sup>78</sup> UNICEF Office of Research – Innocenti (2022a).

<sup>79</sup> Richards et al. (2024).

<sup>80</sup> The two factors demonstrated strong invariance across sex, age and country, indicating consistent measurement across groups. Multidimensional item response theory revealed that the factors were most informative at average trait levels, indicating that the items provided the greatest measurement precision for respondents with moderate levels of online abuse experiences (Richards et al., 2024).

<sup>81</sup> Richards et al. (2024).

Table 3: Two-factor structure of the Disrupting Harm dataset

Factor 1	Factor 2
Risk of sexual exploitation	Risk of sexual harassment and abuse
f) Someone offered me money or gifts in return for sexual images or videos	a) Someone made sexual comments about me
g) Someone shared sexual images of me without my consent	b) Someone sent me sexual images I did not want
h) Someone offered me money or gifts to meet them in person to do something sexual	c) I have been asked to talk about sex or sexual acts with someone when I did not want to
i) Someone threatened or blackmailed me to engage in sexual activities	d) I have been asked by someone to do something sexual that I did not want to
	e) I have been asked for a photo or video showing my private parts when I did not want to

Based on this evidence, we conclude that there are reasonable grounds to classify technology-facilitated CSEA into two categories – exploitation and abuse – and possibly three (exploitation, abuse and harassment). Next, we explore the implications of these findings in the expert interviews, noting any divergence in interpretation and implications for policy and practice.

### 3. INSIGHTS FROM EXPERT INTERVIEWS

Despite the varied ways that technology-facilitated CSEA is understood and defined across different international instruments and by different organisations, the clear steer from the experts interviewed was that this should not detract from the significant strides made over the past decade in recognising, prioritising and addressing technology-facilitated CSEA.

The very fact that technology-facilitated CSEA has been recognised as a significant form of violence experienced by children is an important milestone, achieved in no small part through the increasing attention on data and evidence.<sup>82</sup>

<sup>82</sup> For an in-depth discussion, see Kardefelt-Winther & Maternowska (2020).



## Expert interviews

**Amy Crocker**, (then) Head of Child Protection and Technology at ECPAT International, which was launched in 1990 as a network of 125 civil society organisations in 104 countries dedicated to ending the sexual exploitation of children, based in Bangkok.

**Helen Mason** is Director of Operations, and **Dr Anastasia 'Asia' Shuster** is the Data and Research Manager at Child Helpline International. Child Helpline International has 155 members from 133 countries. Child helplines field over 13 million individual calls each year and provide counselling services to almost 3 million children and young people.

**Professor David Finkelhor** is Director of the Crimes against Children Research Center, Co-Director of the Family Research Laboratory, Professor of Sociology and University Professor at the University of New Hampshire. He co-founded the National Survey of Children's Exposure to Violence (NatSCEV) and the National Incidence Studies of Missing, Abducted, Runaway and Thrownaway Children (NISMAART).

**Professor Deborah Fry** is Professor of International Child Protection Research at the University of Edinburgh and Director of Data for Childlight. Childlight takes a data-driven, evidence-based approach to understanding the prevalence of child sexual exploitation and abuse across the globe, translating data into sustainable action that safeguards children.

**Denton Howard** has been the Executive Director of INHOPE since 2005. INHOPE works with hotline teams in 54 countries to enable the rapid identification and removal of CSAM from the digital world. It supports hotlines and partner organisations through training, best practices, quality assurance and staff welfare.

**Iain Drennan** has been the Executive Director of WeProtect Global Alliance since its launch as an independent international institution in April 2020. WeProtect provides a space for governments, the private sector, and civil society to develop approaches to technology-facilitated CSEA through their Model National Response.

**Michael Tunks** was Head of Policy and Public Affairs of the IWF. The IWF, an independent NGO, identifies and removes global online child sexual abuse imagery. It runs a hotline and works with human analysts to develop tech tools to identify and remove CSAM.

**Dr Najat Maalla M'jid** is the UN's Special Representative of the Secretary-General on Violence against Children (UNSRSG VAC). Her portfolio is broad, covering all forms of violence against children, but with a recent focus on the creation of safer digital environments for children.

**Sean Litton** is Executive Director of the Tech Coalition, an alliance of global technology companies that work together to combat child sexual exploitation and abuse online. It is funded by member companies (i.e., the tech sector), and does not accept funding from any government agency or National Center for Missing & Exploited Children.

This section presents the findings from interviews designed to reveal how high-level stakeholders understand and make sense of classifications and conceptualisations of technology-facilitated CSEA and related risks in their work. We discuss these in relation to three main topics – concepts and definitions, the role of technology, and the role of the child – and show how the six principles emerged from the experts’ insights and commitment to advance a common agenda.

### 3.1 Conceptualising technology-facilitated CSEA

*Substantial inconsistencies in definitions and conceptualisations in studies are creating a research field equalling to a mix of ‘apples and oranges and pineapples.’ Typologies are really, really important because it corresponds to both the legislation and how it’s framed or thought about, but also how all of the online stuff gets enacted upon, which is different than the offline, which is kind of seen in a much more holistic way. (Deborah Fry, interview, 2024)*

The importance of understanding the problem before designing the solution is evident, as is the importance of data and evidence. Inadvertent harm to children may result from inappropriate or poorly designed policy, laws or interventions that fail to take into account the reality of children’s experiences in the digital environment, or their specific collective needs and rights.

However, divergence in concepts and terminology is to be expected in a global and rapidly changing domain. Stakeholders vary in their assessment of how much this matters. As WHO has observed, ‘the lack of clarity and consistency around terminology is likely to persist for a while and is a clear impediment to the accumulation of knowledge and programme development, adaptation and dissemination’.<sup>83</sup> Or as noted by Finkelhor and colleagues: ‘definitional categories are still in flux, and the large variety of concepts being used in research and advocacy have often not been clearly operationalized’.<sup>84</sup>

On the one hand, different actors have varied interests and needs in this changing environment. Conceptual fluidity might allow stakeholders to develop approaches that suit their specific interests and mandates. However, constantly changing terminology can make it difficult for frontline practitioners to address the challenges they face. There are also implications for training and capacity-building, as well as for standard operating protocols, procedures and case management systems. In short, different conceptualisations may offer different utility to different stakeholders, depending on where they sit within the prevention or

---

<sup>83</sup> WHO (2022)

<sup>84</sup> Finkelhor et al. (2023a, p. 8)

response system. This again may differ from how children experience or talk about technology-facilitated CSEA themselves and the language they use to describe their experiences.

For example, legal terminology within any specific context may differ greatly from how children describe their experiences or how social workers, psychologists or other psycho-social professionals categorise and describe children's experiences. This terminology may differ from the language researchers use to define and categorise technology-facilitated CSEA.<sup>85</sup> These differences are often missed in the quest for a common language. At one end of the spectrum might be considered the language and understanding children have; at the other end is that required and used by prosecutors and the judiciary to prosecute such offences. This operational difference in understanding may limit how researchers interpret and analyse data, and how that data is subsequently used for advocacy purposes.

On the other hand, consistent terminology is seen by stakeholders as crucial for making the issue more recognisable and manageable, thereby enhancing the effectiveness of responses from various stakeholders. Consistent terminology is also useful for specific stakeholders including online platforms and law enforcement. Platforms are under increasing pressure to respond proactively to technology-facilitated CSEA and other risks. Consistent terms can help address intermediary and platform liability challenges. Such clarity ensures that platforms understand their obligations and can implement appropriate measures to combat technology-facilitated CSEA. Otherwise, there is a risk that they evade responsibility by hiding behind vague conceptualisations of technology-facilitated CSEA.

Similarly, for law enforcement and prosecution services, consistent terminology is critical for legal certainty. Yet the lack of such certainty should not hinder legal action. Specific legislation to address technology-facilitated CSEA is preferred to ensure appropriate legal responses, yet in its absence existing legislation on child exploitation and abuse can still be applied.<sup>86</sup> This allows for prosecution in serious cases, although it may not be optimal or adequately reflect certain dimensions of the problem.

Therefore, technology-neutral terms and measures are preferable, where possible, although at times specificity is needed about particular digital products and services. This is especially because the exponential rate of innovation contrasts with the world of policy and legislation, which, one interviewee noted, 'tend to move at a glacial pace.' Also noteworthy is what might be called 'definitional fatigue' among stakeholders, exacerbated by the time-consuming nature of these debates and the slow process of implementing changes. While it seems widely accepted that nuances exist, experts asserted that there is a common basis to understanding what technology-facilitated CSEA entails. This shared understanding is vital for operational effectiveness.

---

<sup>85</sup> For examples of differences between jurisdictions, see ECPAT International (2022c).

<sup>86</sup> INTERPOL (2023).

## Conceptual consistency, with flexibility in application

While terminology matters, too much granularity in terminology may result in disproportionate attention to certain risks while neglecting others, it may also become what one expert noted as ‘the perfect being the enemy of the good’.<sup>87</sup> By contrast, a more granular approach to technology-facilitated CSEA underscores the importance of dedicated resources, even while recognising the arguments for a broader focus on violence against children. A lack of understanding of the variety of forms technology-facilitated CSEA among policy makers and practitioners may have devastating adverse effects. For instance, policies and governance mechanisms intended to protect children might also facilitate surveillance technologies and laws, adversely impacting overall children’s rights and human rights.<sup>88</sup>

Despite these differences and challenges with conceptualising technology-facilitated CSEA, consistent trends in CSEA and technology-facilitated CSEA have emerged over the past decade, which can undoubtedly provide the basis and direction for developing responses. As we suggest in Principle 1, recognising children’s experiences of abuse allows us to move beyond the specificities of the technological aspects of the crime to address the harm caused.

It is also important to recognise that most debate around these definitions is significantly Anglocentric. However, contextual, linguistic, cultural and regional differences are crucial in how technology-facilitated CSEA is conceptualised and applied in law and practice. These nuances are not easily translated into other languages and cultures, including those where a significant proportion of the world’s children live. One expert notes ‘[w]e have to find a way to talk about the cultural perspective and the cultural understanding of certain terms’. How definitions are operationalised and implemented in practice depends on the context, even when guidelines are translated into different languages. As described by one expert: ‘You have national legislation that maybe will use different terms... I think at the more granular level, there’s always going to be operational and practical diversity in the way that it’s used’. This is recognised by many of those working across contexts and borders, as another expert put it: ‘we need to make sure ... that in the laws you have definitions but not very strict definitions. To be very clear, to make sure that we can prosecute, but also we can protect children, this is very important...We need at least to make sure that we are speaking the same language.’

---

<sup>87</sup> see also UNICEF Office of Research – Innocenti (2022a).

<sup>88</sup> Kardefelt-Winter et al. (2020a).

## 3.2 Understanding the role of technology in the context of violence, exploitation and abuse

### Beyond online versus offline

Children's lives are interconnected with digital technology from an early age, and their development, education, play and relationships traverse both the physical and digital environments, often with few guardrails. There is a growing consensus that it has become increasingly difficult to differentiate between online and offline contexts. These blurred lines have been highlighted by children, for example in the foreword of the 2023 *Global threat assessment* report written by a child.<sup>89</sup> The impact of online abuse is tangible and significant, leaving victims silenced and isolated, thus challenging the notion that online behaviour is separate from real-life consequences.

Various stakeholders use the term 'online child sexual exploitation and abuse,' although the term 'online' can problematically imply a distinct act of using the internet, which risks reinforcing the now disproven binary nature of the 'online' versus the 'offline.' The term 'online' may also misrepresent the technology used to facilitate CSEA, as non-digital devices are often used and may occur via non-internet-connected technologies.<sup>90</sup> An expansive view of what constitutes the 'online' is frequently adopted by stakeholders in this context to incorporate the use of all forms of communication technology, not just digital. As one of the experts put it, 'we've always had an expansive definition of what constitutes online ... if there is an online dimension there somewhere... It's if there is a screen that's come into play during the process, at whatever point during the process, then that brings it within our remit.'

Also important is that stakeholders increasingly recognise a continuum of exploitation and abuse between the online and offline environments, highlighting that abuse can begin offline and then spread online, for instance through the sharing of images.<sup>91</sup> The fluid movement between online and offline environments complicates the categorisation of the offence or experience, as well as the prevention of and response to abuse.<sup>92</sup> If a service provider deals with abuse cases that involve both online and offline elements, the offline aspect might take precedence due to its *perceived* severity. This can lead to the underreporting of the online elements and a failure to support and care for the victim. As noted by one expert, 'all interactions are going to be mediated by technology', and the imperative to locate technology-facilitated CSEA and its prevention and response within a broader understanding of sexual exploitation and abuse becomes even more apparent.

---

<sup>89</sup> WeProtect Global Alliance (2023).

<sup>90</sup> WHO (2022).

<sup>91</sup> Kardefelt-Winther & Mternowska (2020); Stevenson et al. (2023).

<sup>92</sup> Office of the Special Representative of the Secretary-General on Violence Against Children (2023).

***Like most online harms, many of the victimizations are hybrid, and occur in a combined offline-online context. That's true about bullying, and it's true about sexual abuse (David Finkelhor, interview, 2024)***

Experts discussed this problem in relation to the common perception that online harms are somehow less severe due to the absence of physical harm, although the trauma can be equally devastating.<sup>93</sup> Particularly in resource-constrained contexts, or those characterised by high levels of physical violence or other forms of sexual violence, services may prioritise these over online harms. This prioritisation is influenced by the immediate and visible nature of physical (sexual) violence compared to the more subtle and pervasive impacts of online abuse. This misses the broader point that technology-facilitated CSEA should be seen as *part of* a broader spectrum of violence that children experience.

***There is a perception out there that online harms are not as bad because there's no physical harm being caused. The trauma isn't as great. (Iain Drennan, interview, 2024)***

The perception that online harms are less severe due to the lack of physical harm can influence how resources are allocated and prioritised. Researchers, policymakers and those providing direct services to children, including child helplines, may hold this view. This view may become further entrenched as technology-facilitated CSEA manifests more within the extended reality realm, such as the case recorded by a victim whose avatar was raped in the Metaverse.<sup>94</sup> Policymakers, researchers and practitioners may consider it insulting to treat such instances on a par with the experience of a 'hands-on abuse survivor'. But others argue that this fails to consider the complex nature of violence, how identities are realised in the digital space, or the potential of abuse within these new immersive environments to harm.

Technology-facilitated CSEA contributes to challenges in data collection and analysis and discrepancies between online and offline offences. For instance, unwanted exposure to a sexual image, commonly measured in research on technology-facilitated CSEA, has not traditionally been measured in offline sexual abuse metrics. Nor has it been consistently understood or located in evidence regarding the potential harms that might result for the child, yet it is increasingly adopted as a standardised category of technology-facilitated CSEA.

***There has been some tendency to expand the notion of sexual abuse when we get to the online context. For example, some researchers are counting unwanted exposure to sexual images online as a form of online sexual abuse. But being exposed to an unwanted sexual image in the face-to-face environment has not been counted as a form of sexual abuse, unless it is clearly part of an attempted grooming for sexual abuse sequence. Keep in mind, these online unwanted exposures could be the result of spam or mistakenly clicking on something or a peer thinking mistakenly that the***

---

<sup>93</sup> ECPAT International (2022a).

<sup>94</sup> Sales (2024).

*recipient would like to see this image. To consider all this as online sexual abuse may be a very big expansion of the concept of sexual abuse (David Finkelhor, interview, 2024)*

## Locating technology-facilitated CSEA within broader contexts of violence

Recent literature is increasingly viewing technology-facilitated CSEA as a sub-set of violence against children.<sup>95</sup> For instance in WHO's 2022 report, technology-facilitated CSEA is categorised as a sub-set of violence against children, including cyber-aggression and cyber harassment. Locating technology-facilitated CSEA within a broader violence paradigm will likely enhance the understanding (and empirical testing) of drivers and pathways to technology-facilitated CSEA offending and victimisation that might not otherwise be considered.<sup>96</sup> While this understanding is crucial for developing effective preventive and intervention measures, it does require careful thought and attention paid to how sub-sets are categorised by different stakeholders within the field, and whether and where these terms perhaps need to be differentiated for their varying purposes.

*We've had online child sexual abuse and online child sexual exploitation as two separate subcategories. We've just now merged them together. (Anastasia Shuster, interview, 2024)*

One example here is helplines. Some helplines previously considered sexual exploitation and sexual abuse categories separately in online contexts but have increasingly started grouping them together.<sup>97</sup> The distinction between exploitation and abuse may not have meaningful value for the nature of services and counselling provided by support services and child protection workers, and, unless existing as distinct offences within legislation, for law enforcement and prosecution services either.

Nonetheless, there remains disagreement as to whether all violence that is experienced by children in the digital environment or when using digital technology forms part of a continuum. Instead, some experts argued that there are 'unique elements to technology-facilitated abuse that require distinct approaches.'<sup>98</sup> Some aspects of abuse exist solely online or offline, while others span both realms, necessitating a differentiated approach to each context. Experts pointed out that governments and other actors may underestimate the importance and need to address technology-facilitated CSEA because of digital gaps, for instance in low-income countries. However, some evidence on other forms of online risk, produced by UNICEF, EU Kids Online and Global Kids Online, indicates that once countries reach a point of 50 per cent internet adoption in the general population, there appears to be an increase in children's

---

<sup>95</sup> UNICEF (2023); WHO (2022).

<sup>96</sup> Kardefelt-Winther & Maternowska (2020).

<sup>97</sup> Child Helpline International (2023).

<sup>98</sup> As discussed in Kardefelt-Winther & Maternowska (2020).

exposure to online risk. Low connectivity countries therefore have an opportunity to put in place adequate protection mechanisms now instead of waiting until connectivity increases.<sup>99</sup>

Somewhat different from the notion of a continuum between technology-facilitated CSEA and CSEA, and technology-facilitated CSEA and other forms of violence, is the co-occurrence or co-morbidity of exploitation or abuse (and indeed all forms of violence) in the digital and the physical environment.<sup>100</sup> There is a growing body of evidence on shared vulnerabilities and risk factors for violence against children that occurs in the digital environment and that which occurs offline, as well as the co-occurrence rather than a continuum of CSEA that may be experienced across both the digital and physical environment.<sup>101</sup> This necessitates a holistic approach to child protection that encompasses both online and offline violence, recognising the interconnectedness of online and offline risks and harms, and prioritises the overall safety and well-being of children. There is emerging (yet far less-established) evidence that shows that prevention approaches to violence and sexual violence are yielding positive outcomes for the prevention of technology-facilitated violence, including sexual violence against children.

## Technology-facilitated 'sexual abuse' and 'sexual exploitation' as forms of violence

A recurrent theme in the expert interviews was the location of sexual abuse within a broader framework of violence. As one expert described: 'I think violence is the umbrella ... when we are speaking about violence, ... you have various forms and in various settings. But sexual violence for me is an umbrella that embeds abuse, exploitation, and those are forms [of violence] online and offline ... it's connected and interlinked and generates other forms of violence - mental violence, physical violence.' It has been noted that sexual abuse, whether online or offline, is also multifaceted. Regardless of whether it is experienced online or offline, it may take multiple forms. This emphasises the need for a broader understanding of CSEA as a form of violence, within a framework that encompasses mental, physical, verbal and non-verbal aspects.<sup>102</sup>

Experts discussed sexual exploitation as being seen to be more ambiguous than sexual abuse within the context of technology-facilitated CSEA, as both a pathway or process to the act of abuse and as a form of abuse itself. Exploitation was discussed as a critical component in the phraseology of technology-facilitated CSEA, differing from CSAM, which focuses on abuse material. In many frameworks, exploitation requires an element of exchange, both monetary and non-monetary. Further, exploitation may be understood as the manipulation of a child to produce abusive material, differentiating it from the act of abuse itself. While abuse is understood as the act that is recorded and distributed, exploitation often involves coercion or manipulation. The degree to which exploitation involves an exchange is also somewhat

---

<sup>99</sup> Kardefelt et al. (2020b).

<sup>100</sup> WHO (2022); UNICEF Office of Research – Innocenti (2022a).

<sup>101</sup> UNICEF – Office of Research (2022a); Finkelhor, Turner & Colburn (2023).

<sup>102</sup> WHO (2022).



ambiguous and contested, with some experts noting that the exchange required for exploitation must be financial, while others defined it in to include financial or non-financial (in nature) exchanges. The latter definition aligns with the established literature on sexual exploitation, which emphasises that coercive control can be central to exploitation, where the abuser holds power through authority, social status or emotional manipulation rather than financial means.<sup>103</sup>

The experts point out that this ambiguity and uncertainty in understanding translates into legal approaches in many contexts, whether supporting or potentially undermining successful prosecutions, and the tracking of reliable reporting data.

## The complexity of locating harm in technology-facilitated CSEA

As questions arise about the potential consequences of evolving technology, including technology that might facilitate crimes that appear to be – at face value – ‘victimless’, it is important to highlight the importance of differentiating where harm occurs, and at what level we are targeting responses to technology-facilitated CSEA.

Harm to a child resulting from technology-facilitated CSEA may occur at an individual level or a societal level. Additionally, the potential of ongoing or further distribution of material or content through anonymised networks, peer-to-peer file sharing and multi-platform decentralised services may increase both the risk of harm to children as well as amplifying harm when it is experienced by children.<sup>104</sup>

Criminal laws are adopted to prevent relationships that typically result in negative consequences for those involved, although not always, as exemplified in statutory sex crimes where children involved may not see themselves as victims:

***Some of the especially older youth in these online abuse episodes do not see themselves as being victims because they believed themselves to be in love or a desired relationship with this adult. But these are statutory sex crimes. There is harm not just to the youth who may be exploited by the age and power difference. But there is also harm to society, and to other children because violation of the rules can give permission to other adults to ignore these norms. It's fair to say that we have these laws for good reason. (David Finkelhor, interview, 2024)***

This harm is not always located on an individual, but on a societal level affecting children more generally.

The complexity of technology-facilitated CSEA influences the need for established and effective systems that respond to all forms of CSEA while also requiring more targeted response

---

<sup>103</sup> Reddock et al. (2022); Ricardo & Barker (2008).

<sup>104</sup> Canadian Centre for Child Protection (2024).

measures that consider the multiple environments and ways that harm may be experienced, and additional factors introduced by the technology itself.

## What makes the digital dimension so difficult to address?

The digital environment facilitates abuse through various means, such as multi-platform usage, rapid dissemination of content (e.g., CSAM) and jurisdictional challenges. While there is a growing acceptance of the relationship between technology-facilitated CSEA and CSEA, and the common drivers and vulnerabilities that exist for both, some note that the mechanisms of technology-facilitated CSEA may differ.

The involvement of multiple platforms is a significant issue in technology-facilitated sexual exploitation and abuse. Offenders often use larger platforms to gather contacts and move to less detectable environments like end-to-end encrypted messaging services. This cross-platform activity complicates efforts to identify and restrain perpetrators. Tech companies often only see a small part of the abuse on their platforms, making comprehensive intervention difficult. Even when not moving content across platforms, offenders typically use several platforms simultaneously, making detection and intervention more challenging. According to one expert this platform 'hopping' is now considered a default modus operandi for many perpetrators.

The challenges posed by the image-sharing aspect of technology-facilitated abuse may also warrant emphasis. Technology has accelerated and simplified the non-consensual sharing of abusive content, creating unique challenges that do not have direct offline equivalents unless considering group-based abuse. This third-party element of abuse, where content is shared beyond the initial perpetrator, is particularly prevalent online.

Technology also facilitates additional layers of abuse as content can be endlessly copied and shared, amplifying its impact, even though individuals who view and distribute CSAM online often do not interact with children directly. The longer content is available, the more it is copied, saved and reshared, increasing exposure and potential harm, including re-victimisation.<sup>105</sup> Rapid removal aims to prevent the gradual desensitisation and escalation of offending behaviours. The societal costs of such abuse, including reduced life chances, increased health issues and a higher likelihood of involvement in crime, are well documented.

There is also an argument that anonymity afforded by digital technologies creates different modus operandi for online offending compared offline. Online offenders often use anonymising services, store content remotely and employ various tactics to avoid detection by hiding in the digital crowd. The complexity of tracking and apprehending these offenders is compounded by their use of cloud storage and other technologies to obscure their activities.

---

<sup>105</sup> Childright (2024); ECPAT International (2022a).

Nonetheless there is also a growing body of evidence that points to the similarity between various forms of technology-facilitated sexual exploitation and abuse (in general and against children) and other forms of sexual violence, where the perpetrator is known to the victim.<sup>106</sup> However, this does not factor in the assumed anonymity of those who distribute or share images beyond the initial offence. Given this complexity, it may be useful to differentiate between the initial act of abuse or exploitation and subsequent or resulting harms that may result, which introduce the need for specific responses that extend beyond those required for CSEA.

## Role of emerging technologies

A further complication defining technology-facilitated CSEA is presented by the rapid evolution of technology, which, as noted elsewhere, outpaces the development of legal frameworks, leading to a lack of clarity and consistency in addressing technology-facilitated CSEA. Current legal definitions often fail to encompass new forms of abuse facilitated by technologies like AI and virtual reality (VR). Policymakers and law enforcement agencies struggle to keep up with these advancements, and existing legislation frequently lags behind, necessitating more tech-neutral and future-proof laws. AI-generated imagery presents a complex challenge in the context of CSEA as deepfakes and modified images that blur the lines between reality and fabrication, complicating legal and regulatory responses.

*The legislation is way behind in many aspects of online harms against children and young people. Recent cases around the portrayed sexual violence against child avatars, for example, is very difficult to legislate for, especially as the images may be created based on likenesses of real victims. (Helen Mason, interview, 2024)*

In addition to an extended reality environment, generative AI has introduced a range of opportunities for creating and distributing CSAM content through different mechanisms. These include text-to-image models, image-to-image models and inpainting. While no direct contact with a child victim is required for these processes, materials are easily located and used for these processes, meaning the potential harm to the child remains, and indeed, may be amplified.<sup>107</sup> Indeed, the proliferation of new presentations of technology-facilitated CSEA, primarily through AI technology and virtual environments, has further complicated the victim/victimless argument, with some still questioning whether there is a real 'victim'. Yet the actions and simulations that occur within these environments are typically the product of machine learning and artificial environments trained on actual instances of abuse involving children.<sup>108</sup> Therefore, even though there not a specific individual victim, it is still harmful by

---

<sup>106</sup> Kardefeldt-Winther & Maternowska (2020).

<sup>107</sup> UNGA (2024).

<sup>108</sup> Thiel (2023).

enabling perpetrators to learn about abuse and potentially use this knowledge to commit further offences.<sup>109</sup>

Thus, AI-related abuse and violence can act as gateways to other forms of technology-facilitated CSEA that more directly involve children. Related considerations may also apply to the view that AI-generated CSAM could serve as a 'victimless crime'. However, as the literature suggests, exposure to any CSAM, including AI-generated, may lower the threshold for potential contact offences. Further, exposure to CSAM in any form, or forced exposure to any form of CSEA including artificially generated, may be classified as a criminal offence, depending on national legislative frameworks.<sup>110</sup>

Beyond legislation, practitioners are battling with a lot of the conceptual challenges that virtual and extended realities present. One such examples is the degree to which actions such as sexual assault or abuse occurring in virtual spaces like the Metaverse can be considered or defined as contact offences. There is a tension between what is presented in these virtual environments and practitioners are not in agreement as to the degree to which they represent real offences against children.

*How do I know if it was AI created or not? If I think that looks like a child, then it's a child. (Denton Howard, interview, 2024)*

Moving forward, there is a need for research frameworks (and legislation based on that research) that can adapt to rapid technological changes. This involves creating flexible frameworks to address new forms of abuse as they emerge, perhaps focusing on actions and content rather than the technology itself. Developing comprehensive safety measures, improved data collection and a deeper understanding of how technology facilitates abuse is essential for evolving the response to technology-facilitated CSEA. Enhanced international cooperation and shared best practice will also play a vital role in combating these global challenges. There is widespread recognition that updating legislative and policy frameworks takes time.

### **3.3 Understanding the position of the 'child' in technology-facilitated CSEA**

#### Technology-facilitated CSEA as a catch-all for unwanted sexual activity

Conceptualisations of technology-facilitated CSEA can become muddled insofar as young people engage in exploration of sexuality and intimate relationships facilitated by digital technologies, which can result in novel and escalating risks for harm. These complexities and

---

<sup>109</sup> UNGA (2024).

<sup>110</sup> UNICEF Office of Research – Innocenti (2022a).

tensions, balanced with the imperative to act on a joint agreement of what constitutes technology-facilitated CSEA, point to the importance of considering the experiences of victims of technology-facilitated CSEA as well as stakeholders who work with them, but also considerations of how young people use digital technologies.

Recently, professionals working within both research and implementation have voiced concerns regarding, what they view as the over-criminalisation of behaviours in online contexts compared to offline ones.<sup>111</sup> This is in part due to expansive definitions of technology-facilitated CSEA in recent criminal law, which may criminalise actions online that might not be considered offences offline.<sup>112</sup> This discrepancy challenges law enforcement, which face an expanded scope of responsibilities. Even when intended to protect children, this may inadvertently hinder children's rights to explore their sexuality safely.<sup>113</sup> It has been widely noted that protection regimes tend to prioritise the notion of 'child innocence', potentially neglecting the real needs and rights of children, especially as children get older. Such legislative and regulatory interventions might focus more on public expectations than on the actual wellbeing and rights of individual children.

As noted from the outset of this report, the lack of consistency in definitions and measurements can lead to an inaccurate representation of the prevalence and nature of sexual exploitation and abuse in both online and offline contexts. These various challenges point to the importance of ensuring that definitions and terminology adopted in research, and as operationalised in both practice and policy, do not inadvertently result in the undermining of children's collective rights through mismeasurement or misclassification of children's experiences or the misapplication when operationalising this terminology.

## Child-produced content and age of consent

Finkelhor, Turner and Colburn's study on online sexual offences in the US reveals that a significant proportion (88 per cent) of 'childhood abuse experiences' are produced by youth themselves.<sup>114</sup> Consequently, he suggests rebranding these incidents as 'image-based exploitation and abuse of children' rather than the commonly used term 'child sexual abuse images.' There are many terminological difficulties here. Determining the appropriate response to child-produced content involves complex considerations of developmental and maturity differences across ages and cultures, factors that are rarely considered in standardised measures of technology-facilitated CSEA, nor in legislation or policy. There is a significant challenge in addressing a 14- or 15-year-old consensually sharing sexual images, which may be viewed differently across jurisdictions and contexts.

---

<sup>111</sup> Bulger et al. (2017); Finkelhor et al. (2023c).

<sup>112</sup> Bulger et al. (2017); Finkelhor et al. (2023c).

<sup>113</sup> Bulger et al. (2017); Staksrud et al. (2020); Witting (2022).

<sup>114</sup> Turner & Colburn (2023a).

The issue of consent in the digital environment is complex, particularly regarding child-produced content. In many jurisdictions, a child cannot legally consent, complicating how voluntary content created by children is viewed and regulated. This is further complicated by different age of consent laws across countries. In many countries, 16- to 17-year-olds can legally engage in consensual sexual relationships with peers of a similar age as well as with adults close in age. Such interactions are not considered abuse offline if the adults involved are only slightly older, such as recent high school graduates (with less than a two-year age gap). This discrepancy creates challenges distinguishing between consensual and non-consensual interactions in online contexts. However, even if the age of consent makes certain sexual interactions with children legal, the consensual nature of the interaction needs to be established to avoid the creation of legal loopholes.

### Specific challenges: 'self-generated' sexual content

In the context of technology-facilitated CSEA, it has become increasingly clear that voluntary 'self-generated' content, like so-called 'sexting', is distinguished from content that is created under non-consensual conditions (pressure, taken without consent or shared without consent) or misused or distributed without consent. Although 'sexting' may be illegal in many places, it can take place in a very different context from abusive or exploitative content and requires nuanced understanding and responses. In many countries, law enforcement views consensual sharing between children as less severe, focusing on education and prevention rather than prosecution. However, this approach is not universal.<sup>115</sup> Yet the impact of non-consensual sharing of content can be harmful and is particularly severe when it involves the child's primary social network, leading to significant disruption and stigmatisation. As one expert said: "'Self-generated' itself implies blame on victims. We don't believe that that's the case obviously, but it's just an uncomfortable term.'

There has also been unease at using the term 'self-generated', which is seen as problematic and potentially victim-blaming.<sup>116</sup> This is particularly the case if the child has been coerced or groomed to create imagery of themselves. Despite the consensus on its inappropriateness, there is no widely accepted alternative term. One alternative is to ensure terminology reflects the nuances of abuse facilitated by technology. The concept of 'remote-coerced' abuse was suggested by some of the interviewed experts suggesting it better captures the sequence of contact, initiation and image creation, all considered offences.

Differentiating between consensual and non-consensual child-produced content,<sup>117</sup> recognising the profound impact of non-consensual content and carefully choosing terminology that does not blame victims are essential steps in effectively protecting children in digital environments. Ensuring that these elements are all taken into account, not only by policymakers, legislators

---

<sup>115</sup> See, for example, Council of Europe (2022).

<sup>116</sup> UNGA (2024).

<sup>117</sup> Finkelhor et al. (2023c).

and law enforcement, but also by researchers in the way that data is collected, analysed and presented, is critical in ensuring that appropriate and proportionate responses are formulated.

## Understanding the adult perpetrator

As with contact CSEA, the traditional focus on ‘stranger danger’ in the context of technology-facilitated CSEA may be misguided, as evidence suggests that children are often abused by people they know in their families or community networks, rather than strangers. This has been confirmed by the Disrupting Harm and Global Kids Online studies, among others.<sup>118</sup> As an expert notes, ‘I think that trajectory is very similar to the sort of offline stranger in the bush [...], which isn’t to dismiss stranger sexual violence ... there’s this “stranger danger” bias to our whole discussion about online sexual abuse, whereas much of the new research is really showing how much of it is peer and acquaintance related.’

This should not dismiss the severity of stranger-related sexual violence; indeed, some studies have shown that the results of technology-facilitated CSEA from strangers may be more severe than from those known to the child, but highlights the prevalence of acquaintance-related abuse.<sup>119</sup> Disrupting Harm data shows that stranger perpetrators are more common in some countries than others, and that are particularly common when children experience online sexual abuse on social media platforms.<sup>120</sup> However, this ‘stranger danger’ stereotype skews public perception and policymaking in many contexts.

There is a far smaller body of literature that focuses on other aspects of technology-facilitated CSEA perpetrators, beyond simply the relationship of the perpetrator to the victim, highlighting the importance of expanding this evidence base to better address demand-side drivers to understand what motivates offenders of different forms of technology-facilitated CSEA. Experts also discussed the difficulties in delineating between cases committed by adults and the transgressive behaviours perpetrated by peers.<sup>121</sup> Different motivations and drivers apply, and differentiated responses are required. Understanding the perpetrators of technology-facilitated CSEA in research requires, at a minimum, this level of categorisation.

---

<sup>118</sup> Burton (2024); UNICEF Innocenti – Global Office of Research and Foresight (2023b).

<sup>119</sup> Finkelhor et al. (2024); Wolak et al. (2010).

<sup>120</sup> UNICEF Innocenti – Global Office of Research and Foresight (2023b).

<sup>121</sup> See also <http://globalkidsonline.net/sexual-exploitation-un>

## 4. PRINCIPLES FOR ADDRESSING TECHNOLOGY-FACILITATED CSEA

There is no doubt that our understanding of technology-facilitated CSEA and responses to, all forms of technology-facilitated violence has come far in the last decade, as reflected in the growing body of evidence (more recently including from the Global South through primarily the Global Kids Online and Disrupting Harm studies). Yet, as this report has illustrated, a distinct gap remains between what is being measured and presented as technology-facilitated CSEA, and the level of detail and precision required to adequately legislate and respond in ways that centre the collective and individual rights of children within the framework of the Committee on the Rights of the Child's General comment No. 25 on children's rights in relation to the digital environment.<sup>122</sup>

Based on the findings of this report we propose six child rights centred principles to address technology-facilitated CSEA. These principles can be used by researchers in guiding how it is conceptualised and measured; by policymakers in how they read, understand and translate that research into policy and practice; and by frontline and child protection practitioners in how they develop systems that appropriately and proactively respond and protect those who are the most vulnerable. Further, we believe that a holistic child rights perspective ensures proportionate responses in case of competing children's rights.

The principles aim to enhance the protection of children from all forms of violence, sexual exploitation and abuse, as set out in Articles 19 and 34 of the UNCRC. Further, they aim to enhance children's right to freedom of expression (Article 13), right to privacy (Article 16), right to access to information (Article 17), right to protection from arbitrary deprivation of liberty (Article 37) and the rights of the child in the child justice system (Article 40). These rights should be viewed through the lens of the right to non-discrimination (Article 2), the best interests of the child (Article 3), the right to life, survival and development (Article 6) and the right to be heard (Article 12). This is not an exhaustive list of all children's rights that might be engaged in different scenarios; instead, it points towards those that are the most significant in interpreting and applying the principles.

It is important to stress that all children's rights are interrelated, interdependent and indivisible. This means that none takes precedence over the other. Any restriction of children's rights must have a legal basis, pursue a legitimate aim and be necessary and proportionate. Since measures

---

<sup>122</sup> ECPAT International (2022c); Kardefelt-Winther & Maternowska (2020).



to identify, prevent and combat technology-facilitated CSEA often compete with other children's rights, a careful balancing act of competing rights must be undertaken to ensure the planned measures are proportionate and contribute to realising all children's rights.<sup>123</sup>

## Principle 1: Children's voices count

### Key messages

- **Conduct ethical high-quality research and consultations with a diverse range of children, ensuring their voices are heard.**
- **Children's voices should be used to inform the design of measures to respond to technology-facilitated CSEA.**
- **Evidence generation which centres children's experiences should be embedded and institutionalised into broader processes.**

General comment No. 25 clearly notes the importance of data and evidence generation for policymaking and legislating, and for generating new insights as to children's collective, but also specific, experiences in the digital environment. This aligns with the child's right to be heard, and to their views being given due weight in matters that affect them (Article 12 of the UNCRC). Considering the sensitive nature of technology-facilitated CSEA, both research and consultation with children on this topic needs to follow strict safeguarding protocols and be designed and executed in a way that prevents any adverse impacts on the participating children, centring the principle to do no harm. This means that children's voices should only be included in research projects if the design and execution of the research meets high ethical standards; otherwise, the potential negative impacts of such research may outweigh the benefits of including children's voices in the first place. In this context, researchers should ask children about potential risks they encounter online and the impact, that is, the harm they might experience as a result.<sup>124</sup> This extended focus on risks and harms (with a clear distinction between the two) helps us avoid certain assumptions we, as adults, might have on what is indeed 'harmful' to children.

For consultation to be meaningful, the voices of a diverse range of children should be heard, the questions they are asked should be relevant to their lives and respectful of their experiences, and their ideas and suggestions should indeed be considered in decision-making

---

<sup>123</sup> Livingstone et al. (2024).

<sup>124</sup> Livingstone (2013).

processes.<sup>125</sup> When designing measures to protect children from technology-facilitated CSEA, children's views should be considered to understand better whether such measures have any inadvertent adverse impacts on other areas of children's rights in digital spaces, such as accessing appropriate information, participating in online spaces, or privacy and data protection. Hence, children's voices should not only be considered when defining the problem, but also when designing the solution.

Last, data generation should not be an occasional or one-off endeavour. As technology and children's engagement with digital technology changes, their needs, as well as the risks and harms they may encounter, also change; thus, evidence generation should be embedded and institutionalised into broader processes to develop measures to ensure their relevance. This ongoing research is also required to ensure that the unintentional harm and adverse impacts of interventions, support, policy and legislation do not result from well-meaning initiatives. At the same time, the lack of evidence should not be viewed as an impediment to measures to ensure children are safe from technology-facilitated CSEA.

### Questions for stakeholders to consider

- 1 Have you considered how to include the voices of a diverse group of children meaningfully while upholding safeguarding standards and the do-no-harm principle?
- 2 How can you learn from and design actions in response to children's experiences and views of technology-facilitated CSEA, also carefully contextualising what they say within children's broader experience with digital technologies?
- 3 How can you ensure that children's views are heard by those with the power to make a change, and that research and consultation is not a one-off exercise but institutionalised into a broader process of prevention and response efforts?

## Principle 2: Language matters

### Key messages

- **Follow the advice of the Luxembourg Guidelines and especially avoid using language that blames children.**
- **Adapt the terminology to the context, while embedding universal understandings of behaviours and dynamics that underpin technology-facilitated CSEA.**

<sup>125</sup> Diversity here should be taken to include a wide range of variables, particularly drawing on what we know about those that have been shown to impact children's digital experiences. These include (but are not limited to) socioeconomic status, digital skills, self-efficacy, those with special needs and disabilities and LGBTI groups (Global Kids Online, 2019).

When speaking about children's online experiences, stakeholders should always use language that does not blame children for the actions of others. They should also listen to and understand children's own experiences of all forms of sexual victimisation and the language that they use.

A common language, such as the terminology advised in the Luxembourg Guidelines, benefits the streamlining of research, prevention and response efforts. Noting also the needs of different audiences, regional differences and the pace of technological change, it is critical that definitions and responses to technology-facilitated CSEA remain suitably flexible, so as not to impose a stringent use of agreed terms while ensuring a common understanding of and response to the behaviours and dynamics underpinning the acts and the environments in which they occur.

Note that the understanding and application of technology-facilitated CSEA definitions and terminologies primarily focuses on the English language. These definitions may not translate easily, or at all, into other languages. Many forms of sexual activities and sexual violence do not have ready translations within different linguistic and cultural contexts. Retaining the core understanding of the act and behaviour rather than the definition is important to ensure that a 'universal' core of what constitutes technology-facilitated CSEA is retained. This may be achieved in part through a clear understanding between different disciplinary, service and response professionals of how exploitative and abusive violent behaviours relate to each other.

Stakeholders should also avoid introducing new terms, jargon or acronyms to describe technology-facilitated forms of CSEA. This might lead to 'terminology fatigue' among target audiences, deterring people from engaging in the topic of technology-facilitated CSEA as they might perceive it as a topic that is too complex to understand and tackle.

For advocacy purposes, it may be beneficial to use a term understood by the audience rather than one that is in line with a globally recognised definition. While any form of victim-blaming language should always be avoided, more colloquial terms, or terms that are commonly used to describe technology-facilitated CSEA in a specific age group, might be preferable. If there is scope, stakeholders might explain to the audience why a specific definition of technology-facilitated CSEA is used, as this might help to raise awareness around the importance of language used in this space.

### **Questions for stakeholders to consider**

- 1 Have you familiarised yourself with language commonly used within the specific (country or other) context when speaking about technology-facilitated CSEA, and carefully considered its relation to shared terminology as in the Luxembourg Guidelines?
- 2 Are you avoiding language that can be taken to blame the victim-survivor for the actions of others?

- 3 If using a language other than English, does your terminology capture the common understanding of the behaviours and dynamics that underpin technology-facilitated CSEA?

## Principle 3: Take care with context

### Key messages

- **Recognise the interrelatedness of vulnerabilities and protective factors between CSEA and technology-facilitated CSEA, recognising how these vary by individual and both online and offline contexts.**
- **Locate technology-facilitated CSEA within a broader understanding of offline violence, abuse and exploitation to prevent and mitigate ‘techno-solutionism.’**
- **Recognise that pathways to harm are diverse so that responses to technology-facilitated CSEA should take a case-by-case approach, to ensure the optimal response.**

While technology-facilitated CSEA may assume particular characteristics that relate to the use of digital technology in some aspect or stage of its occurrence or perpetration, technology-facilitated CSEA remains a form of child sexual exploitation and abuse, with associated and common risks and vulnerabilities, across individual, family, community and societies. Recognition of vulnerabilities, strengths, protective factors and capacities across the digital and physical environments is required to ensure the combination of prevention and mitigation that can ensure a streamlined approach to keeping children safe online and offline.

Related to this principle, the nature of how technology-facilitated CSEA occurs and is experienced may vary. Some instances of technology-facilitated CSEA may involve a pathway from CSEA to technology-facilitated CSEA, or vice versa. Some may occur only in the digital environment, while some CSEA may occur without any online component.

Further, CSEA, technology-facilitated CSEA and related harms might manifest concurrently rather than on a continuum. For example, a child might experience severe bullying by peers in school and also experience technology-facilitated CSEA perpetrated by an adult, or online sexual abuse perpetrated by a peer. While there is no continuum between the two risks, as the perpetrators are unrelated, the child might concurrently experience both forms of risk due to specific vulnerability factors and a lack of protective factors.

Therefore, stakeholders should not make any assumptions around particular pathways but should assess each case of technology-facilitated CSEA individually to identify whether there is a continuum or concurrence of harms, or whether it is solely a case of technology-facilitated

CSEA. This case-by-case approach ensures stakeholders identify and address the relevant drivers and risk factors to design case-specific protective measures. Similarly, the assumption that technology-facilitated CSEA always leads to some form of offline CSEA might also diminish the harm experienced by children who exclusively experience technology-facilitated CSEA without any offline component. Therefore, technology-facilitated CSEA and offline CSEA should not automatically be conceptualised as a progression of harms, which could risk indicating that the offline CSEA experience causes more severe harm to the victim.

Locating technology-facilitated CSEA within a wider understanding of violence, abuse and exploitation will also mitigate a reliance on ‘techno-solutionism’ for different forms of technology-facilitated CSEA, the adoption of which, in isolation from broader primary and secondary prevention efforts or wider environmental drivers, will result in a purely responsive rather than preventative approach that fails to address the drivers and risk factors of technology-facilitated CSEA, regardless of the definitions adopted. Instead, it will allow for a more integrated and holistic approach that promotes universal, secondary and tertiary prevention, and response mechanisms that include but are not limited to technical solutions. Prevention is often portrayed as the responsibility of one or two sets of stakeholders – children, parents or schools. Yet violence prevention, more broadly, is a responsibility of all actors in the ecosystem, including governments, service providers, the education system, parents and caregivers.

### **Questions for stakeholders to consider**

- 1 Have you considered how to best locate technology-facilitated CSEA within the wider conceptualisation, prevention and response to violence, exploitation and abuse while considering its specific characteristics?
- 2 Have you made any assumptions regarding specific pathways between the digital and physical environment?
- 3 Have you embedded technical solutions to combat technology-facilitated CSEA within a broader prevention and response framework?

## Principle 4: Avoid blaming children

### Key messages

- **Responses to technology-facilitated CSEA (whether by legislators, law enforcement, social welfare institutions or parents) must avoid placing blame on child victims, both explicitly and implicitly.**
- **Criminalisation of consensual behaviours and acts between peers that are an expression of their sexuality may have significant adverse effects and encroach on children's rights and their evolving capacities.**

Any form of sexual content that is produced, shared or possessed between children is usually taken to constitute technology-facilitated CSEA. This is the case because legislation in many countries states that children cannot give consent to their abuse or exploitation. However, it is important that responses to technology-facilitated CSEA do not place blame on children either by responsabilising them for their victimization, such as in the case of 'self-generated' technology-facilitated CSEA, or over criminalizing older adolescents who consensually share sexual content with peers.

The Luxembourg Guidelines dissuades the use of terms that responsabilise children who are victims of technology-facilitated CSEA. Such examples include instances where children have been coerced or manipulated into producing so-called 'self-generated' sexual content. Evidence indicates that child victims often avoid reporting their victimisation as they feel and are made to feel that they are at fault. Significant efforts have been made by the interagency working group to suggests alternatives to terminology that places blame on child victims, examples include abandoning terms like 'child pornography' and 'child prostitution'. As discussed in this report, terms like 'self-generated' content also sit uncomfortably with experts as it too risks placing blame on child victims, rightly so as in some jurisdictions children have faced criminal liability for producing such content.<sup>126</sup> In many jurisdictions these types of 'self-generated' materials are also framed as less severe, and adults, law enforcement and social welfare services may place blame on the child for producing the content, even if it was the result of manipulation, exploitation or coercion by a perpetrator.

Evidence also reveals that children are often shamed and blamed for their involvement and agency in cases of technology-facilitated CSEA. Child victims have identified this as a significant barrier to reporting. Examples include children chatting with an unknown person online who grooms them, or sending 'self-generated' sexual material to someone they believe is a peer but turns out to be an adult perpetrator. In such cases, children often report feeling ashamed for

<sup>126</sup> ECPAT International (2016), p. 43.

their own actions, which may be confirmed by adult reactions blaming them for what happened. Responses to instances and crimes of technology-facilitated CSEA need to be developed with care to avoid placing blame on child victims, this includes when developing training programs for professionals who work directly with victims.

By contrast it is important to acknowledge that not all sexual content produced and shared by children is abuse or exploitation. When between peers it can be the exploration and/or expression of their sexuality. Mislabelling and any associated potential response, such as criminal penalties, risks criminalising consensual behaviours and acts between peers that may lead to greater harm in the longer term. Treating these as equal in risk and potential severity of harms (if any) to technology-facilitated CSEA perpetrated without consent or by an adult, in research, data presentation, intervention or response, may also lead to a misleading over-estimation of certain forms of technology-facilitated CSEA that undermines the need for a more differentiated and appropriate response. The importance of context cannot be over-emphasised through all these instances.

While children have a right to protection from abuse, their evolving sexuality has never before received so much monitoring as in the digital age, where daily traces are left of browsing history, communications with peers, photo albums and app usage. There is a risk that children's sexuality can become increasingly scrutinised, and even criminalised. The Committee on the Rights of the Child makes it clear that adolescents of similar ages should not be criminalised for consensual sexual activity,<sup>127</sup> and applies the same standard to online sexual activity, stating that 'children should not be held criminally liable for producing images of themselves'.<sup>128</sup> When approaching this complex issue, stakeholders should critically interrogate the age of consent to sexual activity in their respective country context, and assess whether this set age allows enough space for consensual sexual expression of adolescents, and whether it should be any different in the digital environment.

At the same time, the Committee also recognises that in cases where initially consensually produced material is further distributed without the consent of the depicted child, the distributors should be held criminally liable, even where the distributor is a child themselves.<sup>129</sup> In line with the UNCRC, stakeholders should prioritise diversion measures or restorative justice approaches for children in conflict with the law due to technology-facilitated CSEA. Diversion involves referring matters away from the formal criminal justice system, usually to rehabilitation programmes or activities. A restorative child justice approach is an approach in which the victim(s) and offender(s) participate actively together in resolving matters arising from the crime, generally with the help of a facilitator. However, a restorative justice approach

---

<sup>127</sup> UNCRC (2019, para. 73).

<sup>128</sup> UNCRC (2019, para. 67); UN (2021, para. 118).

<sup>129</sup> UNCRC (2019, para. 67).

might not always be appropriate, and its suitability should be informed by an overall assessment of the case and in particular, the views of the child victim.

### Questions for stakeholders to consider

- 1 Have you considered how cases of children's sexual exploration and/or expression are categorised in the context of technology-facilitated CSEA?
- 2 Have you put in place sufficient measures to avoid criminalisation of children for certain forms of consensual production and distribution of sexualised images and videos?
- 3 Have you considered how child offenders of technology-facilitated CSEA will be treated within the child justice system?

## Principle 5: Future proof policy

### Key messages

- **Future proof policies by focusing on the abusive and exploitative behaviours or acts that underpin technology-facilitated rather than focusing on specific technologies, typologies or definitions.**
- **Criminal justice professionals should attempt to exhaust the scope of existing legislation to avoid coming to a standstill if legislation is lagging behind in adopting technology-facilitated CSEA provisions.**

One of the major challenges consistently raised in developing and updating typologies, terminology and definitions of technology-facilitated CSEA is the rapid innovation and changing nature of digital technology, and the impact of, for example, generative AI. By focusing on the abusive and exploitative behaviour or individual act regardless of digital environment – whether fully virtual environments such as the Metaverse, extended reality or the use of generative AI – stakeholders might be able to address technology-facilitated CSEA in the context of emerging technologies without being constantly tied up in efforts to update typologies, terminology and definitions of technology-facilitated CSEA.

For example, any sexual act that would constitute a sexual offence or sexual abuse within the physical environment when it occurs within the metaverse may still constitute an act of sexual violence as defined in the Criminal Code, assuming that it details that such acts regardless of environment constitute a crime. Another example is the use of existing CSAM legislation to address cases of AI-generated CSAM. Since the drafting of the OPSC in the early 2000s, lawmakers debated whether so-called 'virtual' CSAM should fall under the scope of the criminal



law. While this debate mainly focused on drawings of CSAM, for example in the context of Manga, many jurisdictions decided to expand the scope of CSAM laws to cover virtual CSAM. These laws can be leveraged to cover AI-generated CSAM, even though the law itself does not mention the specific technology. However, focusing on the act or behaviour, that is, the generation of CSAM involving a fictional child, should suffice for the criminal justice system to respond to such cases.

It is, of course, crucial that criminal justice professionals act within the remit of the law (the rule of law). However, criminal justice professionals should attempt to exhaust the scope of existing legislation as much as possible to avoid coming to a standstill if legislation is currently awaiting amendment. Regarding the need to ‘future-proof’ legislation, that is, formulating it in a way in which it might be applicable, even for future technological developments, it is crucial to respect the principle of legal certainty. This demands that criminal law clearly describes the conduct that is considered punishable by law: a layperson should be able to understand which conduct is prohibited and regulate their own behaviour accordingly. In conclusion, while legal frameworks should be sufficiently open to interpretation to allow their applicability for future technologies, they need to be sufficiently concrete at the same time to respect the rule of law and the principle of legal certainty.

### **Questions for stakeholders to consider**

- 1 Have you considered how the current legal and policy framework can be applied in the context of emerging technologies, even if the frameworks predate these technologies?
- 2 Does your extended application of the law to emerging technologies respect the rule of law?
- 3 Have you drafted legislation in a way that it might be applicable to future technologies, while making sure it is sufficiently compliant with the principle of legal certainty?

## Principle 6: Embrace a child rights approach

### Key messages

- **Stakeholders should assess the impact of technology-facilitated CSEA-targeted interventions on the full spectrum of children's rights, ensuring proportionate responses in case of competing children's rights.**
- **Child rights centred responses to and strategies to prevent technology-facilitated CSEA should be framed within a wider conceptualisation of violence, exploitation and abuse as well as a wider conceptualisation of a safe and rights-respecting digital environment.**
- **Children's rights should be embedded in the products and services that children use following the principles of Child Rights by Design.<sup>130</sup>**

As noted in Section 4, technology-facilitated CSEA is complex, nuanced and multifaceted. While CSEA is arguably equally complex, the digital technology aspect of technology-facilitated CSEA further exacerbates this complexity, as technology-facilitated CSEA takes place within the complex digital ecosystem. Interventions aimed at preventing or responding to technology-facilitated CSEA, might have inadvertent adverse impacts on other users and even non-users of digital technologies, including children. General comment No. 25 states that 'privacy is vital to children's agency, dignity and safety and for the exercise of their rights'.<sup>131</sup> Stakeholders should therefore avoid a privacy vs safety dichotomy, but rather assess the impact of technology-facilitated CSEA-targeted interventions on other children's rights, such as the right to freedom of expression, the right to privacy and the right to access to information and develop an approach which ensures all engaged rights reach their maximum potential.

Prevention and response to technology-facilitated CSEA is therefore rarely a question of black-and-white, but rather an attempt at manoeuvring in various shades of grey. This might seem daunting, in particular as understanding the digital ecosystem is a big task in and of itself. However, understanding the digital ecosystem, its actors, drivers, dynamics and governance, and how these aspects interact, is crucial to developing technology-facilitated CSEA interventions that are effective in tackling the issue. In the same vein, technology-facilitated CSEA is different to other forms of cybercrime, as it includes vulnerable children who require specific protection and care. Therefore, understanding the dynamics and impacts of

<sup>130</sup> Livingstone & Pothong (2023).

<sup>131</sup> General comment No. (2021, para. 67).

technology-facilitated CSEA is equally important to develop measures that sufficiently protect children from this form of sexual exploitation and abuse.

For this purpose, policymakers and stakeholders should engage with others operating in this space, such as digital rights experts, child protection practitioners, technologists, ICT policymakers and child rights experts. These mutual learning engagements will ensure that technology-facilitated CSEA sits both within a wider conceptualisation of violence, exploitation and abuse (see Principle 2) as well as a wider conceptualisation of a safe and rights-respecting digital environment.

To this should be added the role of digital technology companies as a stakeholder in violence prevention. Tech companies can play a significant role in preventing technology-facilitated CSEA by centring children's rights in the design and development of their products and services rather than only considering the needs and vulnerabilities of children as an afterthought. This proactive approach can help create a safer digital environment and empower children to use technology responsibly. This can include the development of internal policies and processes addressing technology-facilitated CSEA; prioritising technology-facilitated CSEA risk identification and risk mitigation as part of child rights and human rights due diligence; centring the needs and vulnerabilities of children through child rights by design,<sup>132</sup> safety by design and privacy by design approaches; designing reporting mechanism and notice-and-takedown procedures with children's needs in mind; and any other actions that actively prevent a tech companies' products or services being used to commit technology-facilitated CSEA.

### Questions for stakeholders to consider

- 1 Do your interventions have any negative impacts on other children's rights, and have you taken sufficient precautions so that all engaged rights reach their maximum potential?
- 2 Do you have sufficient knowledge about the digital environment and on the dynamics and impact of technology-facilitated CSEA to develop interventions in this space that are effective and minimise adverse impacts on other children's rights?
- 3 Have you engaged relevant stakeholders with complementary expertise to better understand technology-facilitated CSEA and the digital environment in which it takes place?

---

<sup>132</sup> Livingstone & Pothong (2023).

## 5. CONCLUSION

Technology-facilitated forms of CSEA present significant harm to children that, like all forms of violence, impacts on all aspects of their lives, their capacity to thrive and realise their full range of rights, and the wealth of opportunities that digital technology could bring. There has been substantial progress in understanding the changing nature of children's experiences of risks, including sexual risks, in the digital space, and in formulating promising evidence-informed practice to prevent and respond to violence that takes place in, and through, the use of digital technologies.

As a result of this growing body of knowledge, the complexities and nuances of technology-facilitated CSEA are becoming more apparent and are likely to grow as digital technology is further embedded into children's everyday lives. In seeking to understand how we can classify and understand technology-facilitated CSEA, questions abound – such as whether images depict real or fake abuse (as in deepfake AI images), or whether abuse more often associated with adult victims (such as image-based sexual assault or intimate partner abuse) merits a distinct label when applied to children, or whether the focus should be on behaviour, content or technology (or all).

As reflected throughout this report, specific areas warrant particular consideration in how technology-facilitated CSEA against children is conceptualised, measured and integrated into policy, legislation and prevention and response systems. These include:

- Recognising that while technology-facilitated CSEA sits on a continuum of violence, and between the digital and non-digital, there may be specific factors that present in some cases that are unique to technology-facilitated violence that are not present in exclusively contact sexual violence.
- How society talks about violence and sexual violence against children, including CSAM, can impact the lived experiences of children. This is, in turn, influenced by culture and language – for instance, definitions that provide specificity in the English language may not translate into other languages and contexts. Relatedly, experiences and content considered of no or little risk to children may be undesirable or even place children at risk in other contexts.
- How children see, experience and understand their digital encounters, which may objectively be categorised as risks by researchers and adults, may, without context, be misrepresented by adults seeking to develop and prioritise policy responses intended to keep children safe.
- Assumptions of harm, and the likelihood and severity of harm, remain largely that, assumptions, with little research detailing how risks translate into actual harm and how

different environmental factors may influence or impact on harmful outcomes.

While these concerns certainly complicate how technology-facilitated CSEA against children is conceptualised, they by no means limit or undermine the progress made thus far. Instead, they highlight the importance of developing and applying common principles across contexts, languages and cultures, and how research is utilised to develop policy, legislation and systems.

As much as standardised, 'universal' definitions and classifications benefit the streamlining of research, prevention and response efforts, this report shows that, given the needs of different audiences, regional differences and the pace of technological change, it is critical that the conceptualisation of technology-facilitated CSEA remains agile and up to date, while also allowing action where relevant definitions are missing. Rather than enforcing terminology top down, we need common understandings of the behaviours and dynamics (human and technological) that underpin the acts and environments in which they take place. To that end, we have proposed six child rights centred principles geared at supporting existing efforts towards clarity and consensus. Hopefully they can help guide unfolding policy debates and discussions alongside the evolving technologies increasingly implicated in CSEA and related risks.

## 6. REFERENCES

- 5Rights Foundation (2021). Explanatory notes: UNCRC General comment no. 25. [https://5rightsfoundation.com/uploads/ExplanatoryNotes\\_UNCRCGC25.pdf](https://5rightsfoundation.com/uploads/ExplanatoryNotes_UNCRCGC25.pdf)
- ACERWC (African Committee of Experts on the Rights and Welfare of the Child) (2021). General comment No. 7 on Article 27 of the ACRWC: 'Sexual exploitation'. [https://www.acerwc.africa/sites/default/files/2022-09/General-Comment-on-Article-27-of-the-ACRWC\\_English\\_0.pdf](https://www.acerwc.africa/sites/default/files/2022-09/General-Comment-on-Article-27-of-the-ACRWC_English_0.pdf)
- Allmark, P., Boote, J., Chambers, E., Clarke, A., McDonnell, A., Thompson, A., & Tod, AM. (2009). Ethical issues in the use of in-depth interviews: Literature review and discussion. *Research Ethics Review*, 5(2), 48-54. <https://doi.org/10.1177/174701610900500203>
- Bulger, M., Burton, P., O'Neill, B., & Staksrud, E. (2017). Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online. *New Media & Society*, 19(5), 750-764. <https://doi.org/10.1177/1461444816686325>
- Burton, P. (2024). *The digital lives Kazakhstani children: Challenges and opportunities*. UNICEF Kazakhstan, Tirana. [www.unicef.org/kazakhstan/en/press-releases/digital-lives-kazakhstani-children-challenges-and-opportunities](http://www.unicef.org/kazakhstan/en/press-releases/digital-lives-kazakhstani-children-challenges-and-opportunities)
- Canadian Centre for Child Protection (2024). *Experiences of child sexual abuse material survivors. How technology companies' inaction leads to fear, stalking, and harassment*. <https://protectchildren.ca/en/resources-research/experiences-of-child-sexual-abuse-material-survivors-report>
- Child Helpline International (2023). *Online Child Sexual Exploitation and Abuse (OCSEA): An escalating problem that is alarmingly underreported*. <https://childhelplineinternational.org/wp-content/uploads/2023/11/2023-OCSEA-Report.pdf>
- Childlight – Global Child Safety Institute (2023). *Creating a brighter path for children*. <https://childlight.org/sites/default/files/2023-02/Childlight%20Data%20Strategy.pdf>
- Childlight – Global Child Safety Institute (2024). *Into the Light: Childlight global index of child sexual exploitation and abuse prevalence*. <https://childlight.org/sites/default/files/2024-05/into-the-light.pdf>
- Chopin, J., Beauregard, E., & DeLisi, M. (2023). Adverse childhood experience trajectories and individual high risk-behaviors of sexual offenders: A developmental victimology perspective. *Child Abuse & Neglect*, 146, 106457. <https://doi.org/10.1016/j.chiabu.2023.106457>
- Colburn, D., Finkelhor, D., & Turner, H.A. (2023). Help-seeking from websites and police in the aftermath of technology-facilitated victimization. *Journal of Interpersonal Violence*, 1-24. <https://doi.org/10.1177/08862605231186156>

Committee on the Rights of the Child (UNCRC) (2019). Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156.

<https://documents.un.org/doc/undoc/gen/g19/268/13/pdf/g1926813.pdf>

Council of Europe (2007). *Details of Treaty 201. Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse* (CETS No. 201).

[www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=201](http://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=201)

Council of Europe (2022). *Lanzarote Committee: Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse.*

*Implementation report: The protection of children against sexual exploitation and sexual abuse facilitated by information and communications technology (ICTs): Addressing the challenges raised by child self-generated sexual images and/or videos.* <https://rm.coe.int/implementation-report-on-the-2nd-monitoring-round-the-protection-of-ch/1680a619c4>

Dalsklev, M., Cunningham, T., Dempster, M., & Hanna, D. (2021). Childhood physical and sexual abuse as a predictor of reoffending: A systematic review. *Trauma, Violence, & Abuse*, 22(3), 605-618. <https://doi.org/10.1177/1524838019869082>

Della Porta, D. & Keating, M. (eds) (2008). *Approaches and methodologies in the social sciences: A pluralist perspective*. Cambridge University Press.

ECPAT International (2016). *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*. Adopted by the Interagency Working Group in Luxembourg, 28 January 2016. <https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf>

ECPAT International (2020a). *Summary paper on online child sexual exploitation*.

<https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf>

ECPAT International (2022a). *Disrupting harm – Conversations with young survivors about online child sexual exploitation and abuse*. [https://ecpat.org/wp-content/uploads/2023/01/DH\\_Survivors\\_FINAL\\_online.pdf](https://ecpat.org/wp-content/uploads/2023/01/DH_Survivors_FINAL_online.pdf)

[https://ecpat.org/wp-content/uploads/2023/01/DH\\_Survivors\\_FINAL\\_online.pdf](https://ecpat.org/wp-content/uploads/2023/01/DH_Survivors_FINAL_online.pdf)

ECPAT International (2022b). Access to justice and legal remedies for children subjected to online sexual exploitation and abuse. Disrupting Harm Data Insight 3. Global Partnership to End Violence Against Children. [https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-3\\_Final.pdf](https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-3_Final.pdf)

ECPAT International (2022c). *Legislation addressing online child sexual exploitation and abuse*.

Disrupting Harm Data Insight 4. Global Partnership to End Violence Against Children.

<https://safeonline.global/wp-content/uploads/2023/12/Disrupting-Harm-Data-Insight-4-Legislation-addressing-OCSEA.pdf>

ECPAT International (2022d). *Promising government interventions addressing online child sexual exploitation and abuse*. Disrupting Harm Data Insight 5. Global Partnership to End Violence

Against Children. <https://safeonline.global/wp-content/uploads/2023/12/Disrupting-Harm-Data-Insight-5-Promising-Government-Interventions-addressing-OCSEA.pdf>

ECPAT International & UNICEF Office of Research – Innocenti (2022). *Children's disclosures of online sexual exploitation and abuse*. Disrupting Harm Data Insight 2. Global Partnership to End Violence Against Children. [https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-2\\_FinalB.pdf](https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-2_FinalB.pdf)

ECPAT International et al. (2017). *Luxembourg Guidelines, Terminology and Semantics, Interagency Working Group on Sexual Exploitation of Children*. <https://ecpat.org/luxembourg-guidelines>

Finkelhor, D., Ormrod, R. K., & Turner, H. A. (2007). Poly-victimization: A neglected component in child victimization. *Child Abuse & Neglect*, 31(1), 7-26. <https://doi.org/10.1016/j.chiabu.2006.06.008>

Finkelhor, D., Turner, H., & Colburn, D. (2023a). Prevalence of online sexual offenses against children in the US. *JAMA Network Open*, 5(10), e2234471. <https://pubmed.ncbi.nlm.nih.gov/36239942>

Finkelhor, D., Turner, H., & Colburn, D. (2024a). The prevalence of child sexual abuse with online sexual abuse added. *Child Abuse & Neglect*, 149, 106634. <https://doi.org/10.1016/j.chiabu.2024.106634>

Finkelhor, D., Turner, H., Colburn, D., Mitchell, K., & Mathews, B. (2023c). Child sexual abuse images and youth produced images: The varieties of Image-based Sexual Exploitation and Abuse of Children. *Child Abuse & Neglect*, 143, 106269. <https://doi.org/10.1016/j.chiabu.2023.106269>

Finkelhor, D., Cavanaugh, C., Turner, H., Colburn, D., Sutton, S., & Mathews, B. (2024b). When is online sexual solicitation of a minor considered sexual abuse? Recommendations for victim prevalence surveys. *Trauma, Violence, & Abuse*. <https://doi.org/10.1177/15248380241268835>

Ghai, S., Magis-Weinberg, L., Stoilova, M., Livingstone, S., & Orben, A. (2022). Social media and adolescent well-being in the Global South. *Current Opinion in Psychology*, 46, 101318. <https://doi.org/10.1016/j.copsyc.2022.101318>

Ghai, S., Vuorre, M., Kardefelt-Winther, D., Ferguson, A., Kurten, S., Livingstone, S., Przybylski, A. K., & Orben, A. (in preparation). Online sexual risks and harms in Sub-Saharan Africa and Southeast Asia.

Global Kids Online (2019). *Global Kids Online: Comparative Report*, Florence: UNICEF Office of Research – Innocenti.

Government of Kazakhstan, 2023, *Comprehensive Plan on the Protection of Children from Violence, Suicide Prevention and Ensuring their Rights and Well-being for 2023 to 2025*. Kazakhstan: Astana

Government of Tunisia (Ministry of Women, Family, Children and Seniors (MFFES)) and UNICEF Tunisia, 2024. *National Action Plan to End Online Violence Against Children*. Tunisia: Tunis.



- INTERPOL (2023). *Law enforcement capacity in online child sexual exploitation and abuse cases*. Disrupting Harm Data Insight 10. Safe Online. <https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-10-final-151223.pdf>
- ITU (2021). *Pandemic in the Internet Age: From second wave to new normal, recovery, adaptation and resilience*. [www.itu.int/hub/publication/d-pref-ef-pandemic\\_01-2021](http://www.itu.int/hub/publication/d-pref-ef-pandemic_01-2021)
- IWF (2024a). *IWF annual report 2023*. [www.iwf.org.uk/annual-report-2023](http://www.iwf.org.uk/annual-report-2023)
- IWF (2024b). *What has changed in the AI CSAM landscape?* [www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report\\_update-public-jul24v13.pdf](http://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf)
- Kardefelt-Winther, D. & Maternowska, C. (2020). Addressing violence against children online and offline. *Nature Human Behaviour*, 4(3), 227-230. <https://doi.org/10.1038/s41562-019-0791-3>
- Kardefelt-Winther, D., Day, E., Berman, G., Witting, S., & Bose, A. (2020a). *Encryption, privacy and children's right to protection from harm*. UNICEF Office of Innovation – Innocenti Working Paper, WP-2020-14. [www.unicef.org/innocenti/media/3446/file/UNICEF-Encryption-Privacy-Right-Protection-From-Harm-2020.pdf](http://www.unicef.org/innocenti/media/3446/file/UNICEF-Encryption-Privacy-Right-Protection-From-Harm-2020.pdf)
- Kardefelt-Winther, D., Twesigye, R., Zlámál, R., Saeed, M., Smahel, D., Stoilova, M., and Livingstone, S. (2020b). *Digital connectivity during COVID-19: Access to information vital for every child*. Innocenti Research Brief 2020-12. [www.unicef.org/innocenti/documents/digital-connectivity-during-covid-19-access-vital-information-every-child](http://www.unicef.org/innocenti/documents/digital-connectivity-during-covid-19-access-vital-information-every-child)
- Kvale, S. and Brinkmann, S. 2008. *Interviews: Learning the craft of qualitative research interviewing*. 2nd ed., Thousand Oaks, CA: Sage.
- Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child internet safety policy. *Journal of Communication Studies*, 18, 13-28. <https://eprints.lse.ac.uk/62278>
- Livingstone, S. & Pothong, K. (2023). *Child Rights by Design: Guidance for Innovators of Digital Products and Services Used by Children*. Digital Futures Commission, 5Rights Foundation. [https://digitalfuturescommission.org.uk/wp-content/uploads/2023/04/CRbD\\_singles-web.pdf](https://digitalfuturescommission.org.uk/wp-content/uploads/2023/04/CRbD_singles-web.pdf)
- Livingstone, S. & Stoilova, M. (2021). *The 4Cs: Classifying online risk to children*. CO:RE Short Report Series on Key Topics. [www.ssoar.info/ssoar/handle/document/71817](http://www.ssoar.info/ssoar/handle/document/71817)
- Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024). *The best interests of the child in the digital environment*. Digital Futures for Children centre, LSE and 5Rights Foundation. [www.digital-futures-for-children.net/best-interests](http://www.digital-futures-for-children.net/best-interests)
- Martin, P.M., Keskes, H.I., Heni, W., Burton, P., Deliege, A.I., Rabhi, C., & Ayari, R. (2023). From entertainment to extortion: Tunisian children's online experiences. *Child Abuse and Neglect*, 145. <https://doi.org/10.1016/j.chiabu.2023.106405>

- Office of the Special Representative of the Secretary-General on Violence Against Children (2023). *A safer digital environment for children: Now is the time to ACT*. UN Secretary-General. [https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/a\\_safer\\_digital\\_environment\\_for\\_children.pdf](https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/a_safer_digital_environment_for_children.pdf)
- Quayle, E. (2021). Online child sexual exploitation and abuse. In J.M. Brown & M.A.H. Horvath (eds) *The Cambridge handbook of forensic psychology*. Cambridge University Press, pp. 279-290.
- Reddock, R., Reid, S.D., & Nickenig, T. (2022). Child sexual abuse and the complexities of gender, power, and sexuality. *Journal of interpersonal violence*, 37(1-2), NP176-NP208. <https://doi.org/10.1177/0886260520909193>
- Ricardo, C. & Barker, G. (2008). *Men, masculinities, sexual exploitation and sexual violence: A literature review and call for action*. Promundo and MenEngage. <https://resourcecentre.savethechildren.net/pdf/1504.pdf>
- Staksrud, E., Olafsson, K., & Milosevic, T. (2020). Children as crowbar? Justifying censorship on the grounds of child protection. *Nordic Journal of Human Rights*, 38(2), 159-173. <https://doi.org/10.1080/18918131.2020.1777770>
- Thiel, D. (2023). *Identifying and eliminating CSAM in generative ML learning data and models*. Stanford Digital Repository. <https://doi.org/10.25740/kh752sm9123>
- Richards, M., Ghai, S., & Orben, A. (2024). *Psychometric evaluation of online sexual abuse indicators in the UNICEF Disrupting Harm Project*. <https://doi.org/10.17605/OSF.IO/QP6WN>
- Sales, N. (2024). A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future? *The Guardian*, 5 January. [www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta](http://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta)
- Stevenson, J., Krzeczowska, A., Jacobetty, P., & Fry, D. (2023). *Nature of online child sexual exploitation and abuse (CSEA)*. Childlight – Global Child Safety Institute. <https://childlight.org/nature-online-child-sexual-exploitation-and-abuse-csea>
- Stoilova, M., Livingstone, S., & Kardefelt-Winther, D. (2016). Global Kids Online: Researching children's rights globally in the digital age. *Global Studies of Childhood*, 6(4), 455-466. <https://doi.org/10.1177/2043610616676035>
- Stoilova, M., Livingstone, S., & Khazbak, R. (2021). *Investigating risks and opportunities for children in a digital world: A rapid review of the evidence on children's internet use and outcomes*. UNICEF Office of Research – Innocenti. [www.unicef.org/innocenti/reports/investigating-risks-and-opportunities-children-digital-world](http://www.unicef.org/innocenti/reports/investigating-risks-and-opportunities-children-digital-world)
- Stoilova, M., Rahali, M., & Livingstone, S. (2023). *Classifying and responding to online risk to children: Good practice guide*. Insafe helplines and the London School of Economics and Political Science (LSE). [www.lse.ac.uk/business/consulting/reports/classifying-and-responding-to-online-risk-to-children](http://www.lse.ac.uk/business/consulting/reports/classifying-and-responding-to-online-risk-to-children)

Third, A., Kennedy, Ü., Lala, G., Rajan, P., Sardarabady, S., & Tatam, L. (2024). *Protecting children from online grooming. Cross-cultural, qualitative and child-centred data to guide grooming prevention and response*. Young & Resilient Research Centre, Western Sydney University, Safe Online & Save the Children.

[https://resourcecentre.savethechildren.net/pdf/REPORT\\_PROTECTING-CHILDREN\\_FINAL.pdf](https://resourcecentre.savethechildren.net/pdf/REPORT_PROTECTING-CHILDREN_FINAL.pdf)

Turner, H.A., Finkelhor, D., & Colburn, D. (2023). Predictors of online child sexual abuse in a US national sample. *Journal of Interpersonal Violence*, 1-24.

<https://doi.org/10.1177/08862605221149090>

UN (United Nations) (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25). [www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation](http://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation)

UNCRC (United Nations Convention on the Rights of the Child) (2019). *Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* (CRC/C/156).

[www.ohchr.org/en/documents/legal-standards-and-guidelines/crcc156-guidelines-regarding-implementation-optional](http://www.ohchr.org/en/documents/legal-standards-and-guidelines/crcc156-guidelines-regarding-implementation-optional)

UNGA (United Nations General Assembly) (2023a). *Annual report of the Special Representative of the Secretary-General on Violence against Children* (A/HRC/52/61), 11 January. Special Representative of the Secretary-General on Violence Against Children.

[https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/reports\\_hrc/a\\_hrc\\_52\\_61\\_en\\_0.pdf](https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/reports_hrc/a_hrc_52_61_en_0.pdf)

UNGA (2023b). *Annual report of the Special Representative of the Secretary-General on Violence against Children* (A/HRC/52/61), 11 January.

<https://violenceagainstchildren.un.org/content/annual-report-special-representative-secretary-general-violence-against-children-human>

UNGA (2024). *Annual report of the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children* (A/79/122). [https://documents.un.org/symbol-explorer?s=A/79/122&i=A/79/122\\_1723826295191](https://documents.un.org/symbol-explorer?s=A/79/122&i=A/79/122_1723826295191)

UNHRC (United Nations Human Rights Office of the High Commissioner) (2021). *General comment no. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25). [www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation](http://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation)

UNICEF (2023). *International Classification of Violence against Children (ICVAC)*.

<https://data.unicef.org/resources/international-classification-of-violence-against-children>

UNICEF East Asia and Pacific & Centre for Justice and Crime Prevention (2020). *Our lives online: Use of social media by children and adolescents in East Asia – Opportunities, risks and harms*.

[www.unicef.org/eap/reports/our-lives-online](http://www.unicef.org/eap/reports/our-lives-online)

UNICEF Innocenti – Global Office of Research and Foresight (2023a). *The role of social media in facilitating online child sexual exploitation and abuse*. Disrupting Harm Data Insight 7. Safe

Online. <https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-7-EVAC-131223.pdf>

UNICEF Innocenti – Global Office of Research and Foresight (2023b). *Who perpetrates online child sexual exploitation and abuse?* Disrupting Harm Data Insight 8, Safe Online.

<https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf>

UNICEF Innocenti – Global Office of Research and Foresight & ECPAT International (2023). *The role of caregivers in preventing online risks and harms for children.* Disrupting Harm Data Insight 9. Safe Online. <https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-9-151223.pdf>

UNICEF Office of Research – Innocenti (2022a). *The relationship between online and in-person child sexual exploitation and abuse.* Disrupting Harm Data Insight 6. Global Partnership to End Violence Against Children. <https://safeonline.global/wp-content/uploads/2023/12/Disrupting-Harm-Data-Insight-6-Online-In-person-Violence-1.pdf>

UNICEF Office of Research – Innocenti (2022b). Children’s experiences of online sexual exploitation and abuse in 12 countries in Eastern and Southern Africa and Southeast Asia. Disrupting Harm Data Insight 1. Global Partnership to End Violence Against Children. [https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-1\\_Final.pdf](https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-1_Final.pdf)

UNICEF Zimbabwe and the Ministry of Information Communication Technology, Postal and Courier Services (2021), National Child Online Protection Policy. Unpublished paper.

WeProtect Global Alliance (2023). *Global threat assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response.* [www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf](http://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf)

WHO (World Health Organization) (2022). *What works to prevent violence against children online?* <https://iris.who.int/bitstream/handle/10665/364706/9789240062061-eng.pdf?sequence=1>

Witting, S.K. (2022). *A commentary on the United Nations Convention on the Rights of the Child, Optional Protocol 2.* Brill Nijhoff, 10 November. <https://doi.org/10.1163/9789004460393>

Wolak, J., Finkelhor, D., Mitchell, K.J., & Ybarra, M.L. (2008). Online ‘predators’ and their victims: Myths, realities, and implications for prevention and treatment. *American Psychologist*, 63(2), 111-128. <https://doi.org/10.1037/0003-066X.63.2.111>

Wortley, R., Findlater, D., Baily, A., & Zuhair, D. (2024). Accessing child sexual abuse material: Pathways to offending and online behaviour. *Child Abuse & Neglect*, 154, 106936. <https://doi.org/10.1016/j.chiabu.2024.106936>



# DIGITAL FUTURES FOR CHILDREN

Research at LSE and 5Rights Foundation ■

**digital-futures-for-children.net**  
**info@dfc-centre.net**

@5RightsFound @MediaLSE  
#DFC #DigitalFutures4Children



THE LONDON SCHOOL  
OF ECONOMICS AND  
POLITICAL SCIENCE ■



**5RIGHTS  
FOUNDATION**

The Digital Futures for Children centre acknowledges funding from the 5Rights Foundation.

This joint LSE and 5Rights research centre supports an evidence base for advocacy, facilitates dialogue between academics and policymakers and amplifies children's voices, following the UN Committee on the Rights of the Child's General comment No. 25.

Creative Commons licence (CC BY-NC)

Please cite this report as: van der Spuy, A., Witting, S., Burton, P., Day, E., Livingstone, S. & Sylwander, K.R. (2024). *Guiding principles for addressing technology-facilitated child sexual exploitation and abuse*. Digital Futures for Children centre, LSE and 5Rights Foundation.

Images: Ron Lach on Pexels