

Legislating for the digital age

Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse



Federal Ministry
for Economic Cooperation
and Development

giz

Deutsche Gesellschaft für
Internationale Zusammenarbeit

Disclaimer: This Global Guide is provided for general informational purposes only. The Global Guide does not contain legal advice and should not be relied upon as such. In certain instances, research and analysis of Laws and Bills were completed by researchers not registered to practice in the jurisdictions to which those Laws or Bills relate and unofficial translations of the texts have, in some instances, been relied upon. While the authors have endeavoured to verify the contemporaneity and accuracy of the Laws and Bills when developing and finalizing this Global Guide, it is possible that the Laws and Bills have undergone amendments which are not reflected in this Global Guide.

Suggested citation: United Nations Children's Fund (2022) *'Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse'* UNICEF, New York.

Published by UNICEF Child Protection Team, Programme Group, 3 United Nations Plaza, New York, NY 10017. Email: childprotection@unicef.org. Website: www.unicef.org.

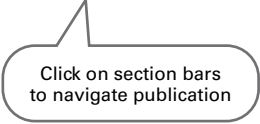
© United Nations Children's Fund (UNICEF) May 2022.

Permission is required to reproduce any part of this publication. Permission will be freely granted to educational or non-profit organizations. For more information on usage rights, please contact: nyhqdoc.permit@unicef.org.

Design and layout: Steve Caplin

Cover Photo: © UNICEF/UNI358624/Cristofolletti





Click on section bars
to navigate publication

Contents

Acknowledgments	2
Acronyms	3
Executive summary	5
1. Introduction	10
2. Consolidated checklist	24
3. Evidence-based legislation	30
4. Stakeholder engagement and catalysts for legal reform	42
5. Methods of legislative reform	50
6. Criminalization of online child sexual exploitation and abuse	54
7. Duties and responsibilities in relation to business	85
8. Procedures and methods of investigation of online child sexual exploitation and abuse	113
9. Victim support, rehabilitation, reintegration and redress	140
10. Independent monitoring and regulation	155
11. Implementation of legislation	160
12. Glossary	168

List of figures

Figure 1: Lundy Model of Child Participation	35
Figure 2: Internet Value Chain	86
Figure 3: Membership of Virtual Global Task Force	115
Figure 4: Procedure on receiving a report of online child sexual exploitation and abuse	125

Acknowledgments

This Global Guide was written by Professor Dame Carolyn Hamilton, Awaz Raof, Catherine Burke and Ramyah Harrichandiran from Coram International. Jorun Arndt, Farah Elhouni and Rosalie Lord from Coram International provided support for the development and publication of this Global Guide. Coram International is a research and consultancy organization dedicated to the promotion and protection of children's rights. Further information about the organization can be found at www.coraminternational.org.



This Global Guide was commissioned by UNICEF to support the work of the Child Protection Programme Team in UNICEF's Programme Group. Afroz Kaviani Johnson, Child Protection Specialist, and Stephen Blight, Senior Child Protection Adviser, oversaw its development and provided technical guidance and support to the authors.

UNICEF gratefully acknowledges the financial support of the Deutsche Gesellschaft für Internationale Zusammenarbeit (BMZ) and the technical support of the German Agency for International Cooperation (GIZ) for this initiative.



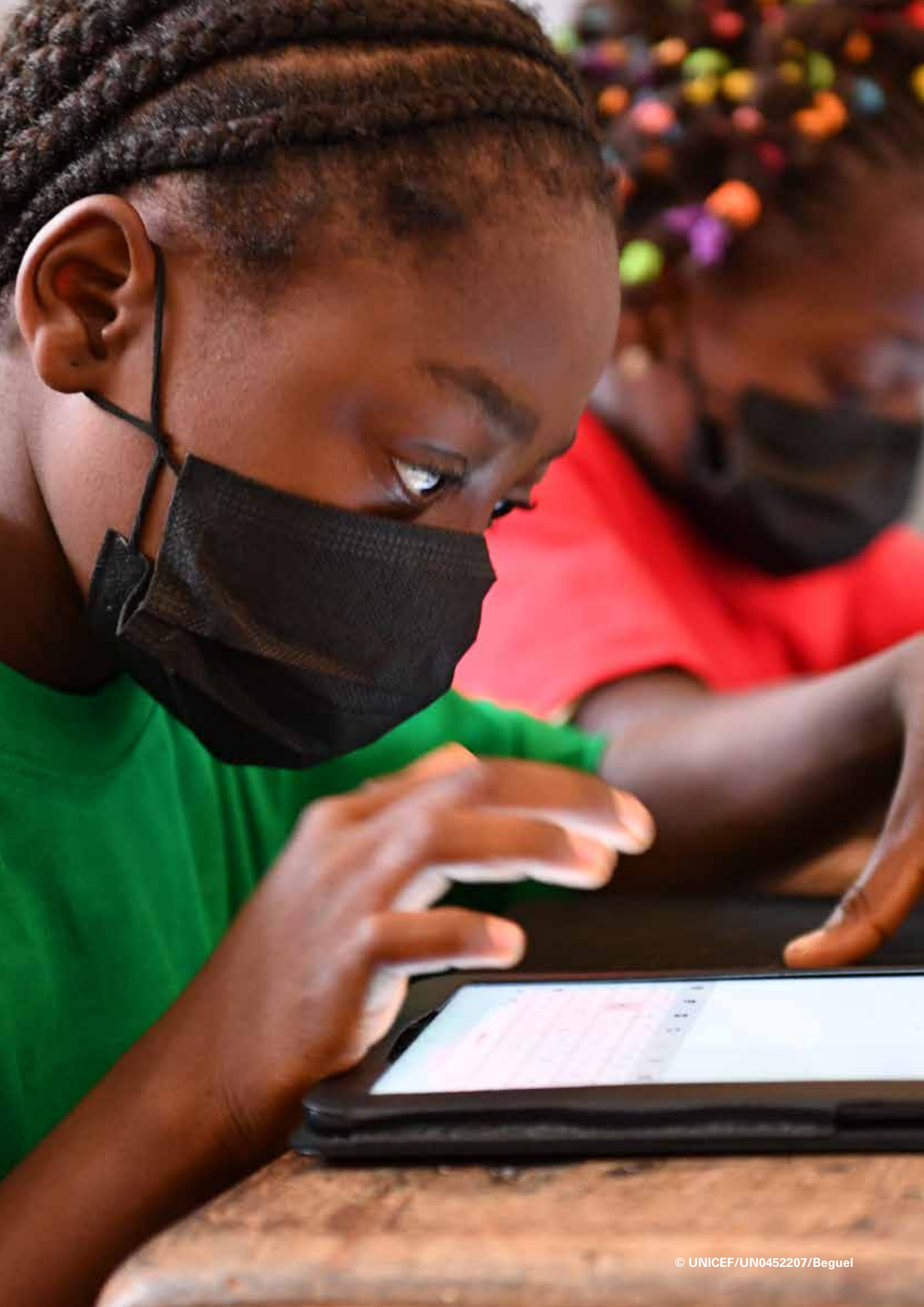
Sincere appreciation is extended to all colleagues, partners and stakeholders who participated in the consultations on the development of this Global Guide, commented on draft versions, and shared their experiences and expertise in protecting children from online sexual exploitation and abuse.

Their insights played a valuable role in informing the guide. These include:

5Rights, Australian Federal Police, Childline Zimbabwe, Crown Prosecution Service for England and Wales, Cyber Crime Unit and Digital Forensics Laboratory of the Criminal Investigations Department of the Ghana Police Service, Cyber Security Authority of the Ministry of Communications and Digitalisation of the Government of Ghana, Department of Home Affairs of the Government of Australia, Department of Infrastructure, Transport, Regional Development and Communications of the Australian Government, ECPAT International, eSafety Commissioner of Australia, European Union Internet Forum, Global Partnership to End Violence against Children, GSMA, Home Office of the Government of the United Kingdom, INHOPE, Inter-Agency Council Against Child Pornography of the Government of the Philippines, International Centre for Missing and Exploited Children, International Justice Mission, International Telecommunication Union, Internet Watch Foundation, INTERPOL, Justice for Children in Zimbabwe, Korea Legislation Research Institute, National Center for Missing and Exploited Children, Office of Cybercrime of the Department of Justice of the Government of the Philippines, Police Scotland, Technology Coalition, UNICEF Argentina, UNICEF Brazil, UNICEF Colombia, UNICEF Costa Rica, UNICEF Dominican Republic, UNICEF East Asia and Pacific Regional Office, UNICEF Eastern and Southern Africa Regional Office, UNICEF Egypt, UNICEF Ghana, UNICEF Gulf Area Office, UNICEF India, UNICEF Latin America and Caribbean Regional Office, UNICEF Middle East and North Africa Regional Office, UNICEF Namibia, UNICEF Office of Global Insight and Policy, UNICEF Office of Research, UNICEF Philippines, UNICEF Programme Group Leadership Team, UNICEF Programme Team, UNICEF Tunisia, UNICEF Zimbabwe, United Kingdom Council for Internet Safety, and the WeProtect Global Alliance.

Acronyms

ACRWC	African Charter on the Rights and Welfare of the Child
ACRWC Committee	African Committee of Experts on the Rights and Welfare of the Child
ACRWC GC 7	General Comment No. 7 of 2021 of the African Committee of Experts on the Rights and Welfare of the Child
ASEAN	Association of Southeast Asian Nations
Covid-19	Coronavirus (SARS-CoV-2)
CRC	Convention on the Rights of the Child
CRC Committee	UN Committee on the Rights of the Child
ECOSOC	UN Economic and Social Council
EU	European Union
GDPR	General Data Protection Regulation
ICMEC	International Centre for Missing and Exploited Children
ICT	Information and communication technology/ies
ILO	The International Labour Organization
INTERPOL	International Criminal Police Organization
ISPs	Internet service providers
IWF	Internet Watch Foundation
LAN	Local area network
MLA	Mutual legal assistance
NCMEC	National Center for Missing and Exploited Children
NHRI/s	National Human Rights Institution/s
NGOs	Non-governmental organizations
NTD	Notice and takedown
OPSC	Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography
OPSC Guidelines	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
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
UNICEF	United Nations Children's Fund
URL	Uniform Resource Locators
USA	United States of America



Executive summary

Rationale and background

The purpose of the Global Guide is to provide guidance on how to strengthen legislative frameworks to protect children from online sexual exploitation and abuse in accordance with international and regional conventions, general comments and guidelines of treaty bodies, model laws and good practices. It is intended for use by governments, country offices of international organizations, civil society and business organizations to assist in ensuring that all aspects of online sexual exploitation and abuse of children are explained and contained in legislation, in line with international and regional standards and good practices.

While the digital environment may provide ‘*new opportunities*’ for the realization of children’s rights, it also presents risks,¹ and ‘*may open up new ways to perpetrate violence against children, by facilitating situations in which children experience violence and/or may be influenced to do harm to themselves or others.*’² Year on year, there are increasing reports of various forms of online child sexual exploitation and abuse. The reported increase in the scale, severity and complexity of online child sexual abuse and exploitation, particularly during the Covid-19 pandemic, is also of particular concern.³ For example, in 2021, the USA-based National Center for Missing and Exploited Children received 29.3 million reports of suspected child sexual exploitation, an increase of 35 per cent from 2020.⁴

The true extent of child online sexual abuse and exploitation, however, remains unknown, in part due to barriers to disclosure and reporting. Interviews with children across 12 countries in the East Asia and Pacific and Eastern and Southern Africa regions during 2020-2021 indicated that between one to 20 per cent of children suffered online sexual

exploitation and abuse in the past year, one in three of whom did not tell anyone about this experience.⁵

Article 34 of the Convention on the Rights of the Child places an obligation on States parties to protect the child from all forms of sexual exploitation and sexual abuse, including all forms of online sexual exploitation and abuse. The Committee on the Rights of the Child has also affirmed that States parties should regularly review, update and enforce robust legislative frameworks ‘*to protect children from recognised and emerging risks of all forms of violence in the digital environment*’ including sexual exploitation and abuse.⁶



The Global Guide uses the phrase ‘*online child sexual exploitation and abuse*’ to describe child sexual exploitation and abuse that is facilitated by information and communication technologies, though the limitations of this term are acknowledged. Further, given that the distinction between ‘*online*’ and ‘*offline*’ is often blurred,⁷ much of the material contained in the Global Guide is also relevant to child sexual exploitation and abuse that is not facilitated by the use of information and communication technologies (i.e. ‘*offline*’ child sexual abuse and exploitation).

Updating legislative frameworks for the digital age

The use of new, rapidly changing digital technologies to sexually exploit and abuse children, the wide reach of online services and the fact that such exploitation and abuse may involve victims and perpetrators from different jurisdictions, all pose challenges to States seeking to protect their children. Many States have yet to put in place or update the wide-ranging legislation that is required to deal with this phenomenon. The protection of children from online sexual exploitation and abuse through legislative measures requires at the very least:

- criminalization of online sexual exploitation and abuse and enforcement of those laws;
- new procedures for investigation, storage and preservation of electronic evidence;
- the regulation of businesses in the digital environment;
- child protection services for victims of online sexual exploitation and abuse;
- access to redress for child victims; and
- independent monitoring of children's rights to protection in the digital environment.

States also need to legislate for new infrastructures, such as a central contact point to receive referrals,

leads and tips regarding suspected cases (including CyberTip referrals from the National Center for Missing and Exploited Children), specialist police and prosecutorial units to follow up referrals, as well as connection to a child abuse image database, access to forensic laboratories, the provision of support services for victims, and training of police, prosecutors, judiciary and other relevant professionals and practitioners.

In addition, States will need to develop secondary legislation to ensure implementation of the newly developed laws.

In the context of many low- and middle-income countries, where fundamental child protection and justice capacities may be constrained, there is a need to strengthen basic structures and systems for protecting children from violence and integrate the specificities of responding to online child sexual exploitation and abuse within these broader frameworks. Indeed, UNICEF's programmatic learning in this field has reiterated the importance of ensuring that online sexual abuse and exploitation are not addressed in isolation, but rather integrated into broader responses to violence against children and child protection efforts more broadly.⁸

Overview of the guide

The Global Guide contains 11 parts. The introduction in **Part 1** sets out the challenges faced by governments and the duty on the State to ensure that adequate legislation is in place to prevent, counter and address online child sexual exploitation and abuse. The introduction also sets out the structure and the major legal instruments that form the framework for the Global Guide and provides definitions and terminology.

Part 2 sets out the key standards which States should address in their legislation. It is important to

States are encouraged to integrate higher standards for the protection of human rights which go above and beyond their minimum obligations under international and regional conventions.

emphasize, however, that States are encouraged to integrate higher standards for the protection of human rights which go above and beyond their minimum obligations under international and regional conventions.⁹

Part 3 deals with evidence-based legislation and the need to ensure that the State has high quality data on the trends and prevalence of child sexual exploitation and abuse to assist it in drafting legislation that focuses on children's lived experiences and the 'harms' caused by online sexual exploitation and abuse. The part provides examples of good practice which States can draw on including mechanisms for integrating the views of children in the development of legislation.

Part 4 provides guidance on the legislative reform process, including potential entry points, techniques for engaging legislators, policymakers and other key stakeholders.

Part 5 reviews methods of legislative reform, and the framework within which new legislation can be introduced. This may be through a criminal justice framework, a cybersecurity law or a child rights or child protection law. The part considers some examples and the opportunities and challenges associated with these different strategies.

The criminalization of online sexual exploitation and abuse forms part of a State party's obligation to protect children under Article 34 of the Convention on the Rights of the Child, while the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, requires States parties to ensure as a minimum that certain acts and activities are criminalized. **Part 6** sets out the offences relating to online sexual exploitation and abuse which States parties are either required to integrate into their legislative frameworks or which are recommended under international and regional standards. It covers offences relating to the production, offering, distribution, dissemination, importing and exporting of child sexual abuse material, accessing or interacting with child sexual abuse material online, online sexual extortion of a child, online grooming of a child, offences to account for new or emerging issues such as 'cyberflashing' and 'cyberstalking' and guidance on how to handle complex issues such as self-generated sexual material.

Part 7 addresses the duties and responsibilities of businesses and the private sector in protecting

children from online sexual exploitation and abuse. Businesses providing content rights, connectivity, user interfaces and online services (for example, e-commerce, entertainment, search services, social and community platforms, cloud and other e-services) are key stakeholders in the digital environment and are integral to protecting children from online child sexual exploitation and abuse. Enabling platforms, advertising services and managed bandwidth and content delivery providers also play an important role. The part emphasizes the need to place child rights at the core in developing legislation and examines approaches to online safety in recent legislative reforms and proposals in Australia and the UK, respectively. It also addresses issues such as age assurance, notice and takedown procedures and the detection, blocking and removal of child sexual abuse materials.

The investigation and prosecution of online child sexual exploitation and abuse raises a number of novel procedural and evidential issues due to the electronic nature of the evidence, the particular problems presented by the obtaining, retention and storage of evidence and the fact that the victim may be in a different jurisdiction to the perpetrator or even to the jurisdiction that identifies and reports the exploitation and abuse. **Part 8** deals with powers and procedures that need to be put into legislation, and the use of undercover investigations, child abuse image databases and obtaining evidence from other jurisdictions through mutual legal assistance.

Article 39 of the Convention on the Rights of the Child requires State parties to *'take all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim.'* The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography further provides that States parties shall ensure that all child victims have access to adequate procedures to seek compensation for the offences committed against them. **Part 9** examines what should be provided in terms of support services and how children can access compensation through the justice system or State-run compensation schemes, as well as their limitations.

Part 10 of the Guide outlines the important role that independent monitoring and regulation of the digital environment plays in protecting children from online sexual exploitation and abuse and the need to integrate children's rights to protection in the digital environment into the legislative mandate and activities of the State's national human rights institution for children.

Looking forward

Putting in place the many building blocks necessary to ensure effective protection from online sexual abuse and exploitation globally is a challenge. It is a challenge that requires:

- political will to address it;
- the introduction of new legislation to criminalize and regulate the online environment to keep children safe;
- the establishment of specialist infrastructure and specialist capacity building in law enforcement and a range of other bodies;
- public awareness raising;
- ongoing training for those implementing the law; and
- an effective child protection system for the victims of child sexual abuse and exploitation.

Adequate financial and human resources are also essential. Putting in place such measures globally will clearly take time.

The aim of this Guide is to provide a starting point: to set out the essential foundations of the building

The aim of this Guide is to provide a starting point: to set out the essential foundations of the building blocks and to provide examples and assistance on how and where to start.

blocks and to provide examples and assistance on how and where to start. Most governments have taken initial steps but those who have advanced further can provide valuable help and insight to others just starting on the process, particularly in relation to some of the more difficult debates

Finally, **Part 11** deals with the implementation of primary legislation to address online child sexual exploitation and abuse, the need to develop secondary legislation to ensure effective implementation and to raise awareness and educate, particularly children, parents, carers and law enforcement authorities, on its contents.

relating to the nature and content of necessary legislation, privacy and protection and the responsibility of the online business sector to keep children safe. International cooperation is also key, given the multi-jurisdictional nature of online sexual exploitation and abuse. New instruments that make it easier for States to access data from one another, as proposed by the new Second Additional Protocol to the Convention on Cybercrime (the Budapest Convention)¹⁰ for example, are to be welcomed.

International cooperation through the provision of databases and training on investigation and new technologies has increased the ability of law enforcement in an increasing number of countries to prevent and prosecute offenders. At present, however, such cooperation has not extended to all countries and there is an urgent need for cooperation to be extended to ensure that there is no possibility of impunity for those that carry out child sexual abuse or exploitation or those that facilitate it, whether knowingly or unintentionally.

Addressing online child sexual abuse and exploitation also requires a well-resourced child protection system that can provide support and services to children that cooperates and works closely with national law enforcement.

The digital environment is ever changing such that new ways and measures to prevent online child sexual abuse and exploitation need to be developed to address this. There is a continuing need for ongoing international and regional research on the impact of the digital environment on children to assist national governments to craft the necessary policy, legislative and practice responses.

Endnotes

- 1 Committee on the Rights of the Child (CRC Committee), General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021 (CRC General Comment No. 25 (2021)), para. 3.
- 2 CRC General Comment No. 25 (2021), para. 80.
- 3 EUROPOL, Covid-19 Sparks Upward Trend in Cybercrime, Press Release, 5 October 2020, <www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime>, accessed 28 September 2021; INTERPOL, Threats and Trends: Child Sexual Exploitation and Abuse – Covid Impact, September 2020.
- 4 National Center for Missing and Exploited Children, CyberTipline 2021 Report, <www.missingkids.org/gethelpnow/cybertipline/cybertipline-data>, accessed 10 May 2022.
- 5 United Nations Children's Fund (UNICEF) Office of Research - Innocenti, Children's experiences of online child sexual exploitation and abuse in 12 countries in Eastern and Southern Africa and Southeast Asia, Disrupting Harm Data Insights, Global Partnership to End Violence Against Children (forthcoming).
- 6 CRC General Comment No. 25 (2021), para. 82.
- 7 Interagency Working Group, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), ECPAT International and ECPAT Luxembourg, 2016, p. 28, www.ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf (ENG), accessed 5 January 2022.
- 8 UNICEF, Ending Online Child Sexual Exploitation and Abuse: Lessons learned and promising practices in low and middle income countries, UNICEF, New York, December 2021, p. 10.
- 9 For example, Article 41 of the Convention on the Rights of the Child provides that, 'Nothing in the present Convention shall affect any provisions which are more conducive to the realization of the rights of the child and which may be contained in: (a) The law of a State party; or (b) International law in force for that State.'
- 10 Council of Europe, Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe, Strasbourg, 17 November 2021, <<https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe>>, accessed 12 May 2022.

1. Introduction

1.1 Purpose of the Global Guide

This Global Guide provides guidance on how to strengthen legislative frameworks to protect children from online child sexual exploitation and abuse.

It is intended for use by governments, country offices of international organizations, civil society and business organizations to advocate for and develop legislation to protect children from online child sexual exploitation and abuse in line with international child rights standards.

This Global Guide is based on the Convention on the Rights of the Child (CRC), the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC), as well as other international and regional conventions, general comments and guidelines of treaty bodies, model laws and good practices concerning the protection of children from online child sexual exploitation and abuse.

1.2 Context

The ‘*digital environment*,’ as it is referred to by the UN Committee on the Rights of the Child (the CRC Committee), has increasingly become an important part of children’s lives.¹¹ The Covid-19 pandemic has reinforced and increased the reliance on and importance of the internet and information and communication technology (ICT) in children’s lives, as lockdowns of schools and other communal areas have pushed routine face-to-face interactions online.¹²

While the digital environment may provide ‘*new opportunities*’ for the realization of children’s rights, it also presents risks.¹³ The digital environment ‘*may open up new ways to perpetrate violence against children, by facilitating situations in which children experience violence and/or may be influenced to do harm to themselves or others*’.¹⁴

An area of specific concern is the use of the internet and other forms of ICTs to sexually exploit and abuse children, referred to in this Global Guide as ‘*online child sexual exploitation and abuse*.’



This Global Guide uses the phrase ‘*online child sexual exploitation and abuse*’ to describe child sexual exploitation and abuse that is facilitated by information and communication technologies, though the limitations of this term are acknowledged. Further, given that the distinction between ‘*online*’ and ‘*offline*’ is often blurred,¹⁵ much of the material contained in this Guide is also relevant to child sexual exploitation and abuse that is not facilitated by the use of information and communication technologies (i.e. ‘*offline*’ child sexual exploitation and abuse).

A robust legal framework is necessary to respond to all forms of child sexual exploitation and abuse, inclusive of those forms facilitated by information and communication technologies. UNICEF’s programmatic learning in this field has reiterated the importance of ensuring that online sexual abuse and exploitation is not addressed in isolation, but rather is integrated into responses to combat violence against children and child protection efforts more broadly.¹⁶

Online child sexual exploitation and abuse may occur in various ways, including through the use of ICTs to solicit children for sexual purposes; live-streaming of the sexual abuse of a child; producing, distributing, viewing or possessing child sexual abuse material online; sexual extortion of a child through the use of ICTs and online grooming, among others.

The International Centre for Missing and Exploited Children (ICMEC) reports that the internet and ICTs *'have created a new dimension in which the sexual exploitation of children can flourish if unchecked'*.¹⁷ Perpetrators may also take advantage of and *'hide'* behind online anonymity when committing abuse or exploitation.¹⁸ As ICMEC has highlighted in relation to child sexual abuse material, the internet not only makes this form of violence *'both easy and inexpensive'*, but it has also made it *'extremely low-risk, enormously profitable, and unhindered by geographical boundaries'*.¹⁹

Practically speaking, children may be *'unsupervised or minimally supervised when online'* and may be more willing to share information and *'trust that the person with whom they are interacting [online] is a friend'*.²⁰ This may, in turn, lead to the child feeling pressured or manipulated into engaging in sexual activities when using ICTs, leading to situations of abuse or exploitation.²¹

Investigations of online child sexual abuse and exploitation rely on the timely detection of such forms of violence and access to reporting mechanisms through which relevant authorities can be notified of such cases. Investigation of online child sexual exploitation and abuse also relies on stakeholders in the private sector who are involved in ICTs, including internet service providers (ISPs), mobile phone operators and social media companies, being willing and able to retain and share data with authorities. Particularly in the area of legislative reform, such discussions may raise complex issues relating to users' rights to privacy and data protection and the basis and scope of limitations to these rights.

Online child sexual exploitation and abuse may take place across multiple jurisdictions, where

the perpetrator(s) and victim(s) are located in different States operating different laws. These disparities lead to challenges, including identifying the jurisdiction in which the online child sexual exploitation and abuse occurred.

Legislative differences on combating online child sexual abuse and exploitation between States weakens the response to child sexual exploitation and abuse, *'allowing offenders to focus their efforts in countries where they know they will not be punished or where laws or prosecution of these crimes are weaker'*.²² Legislative differences also raise practical challenges to the investigation and prosecution of cross-border instances of online child sexual exploitation and abuse due to inconsistent criminal procedure rules.

The investigation and prosecution of online child sexual exploitation and abuse requires law enforcement, prosecutors and judicial bodies to have specialist expertise in both cybercrime and child protection. It also requires clear national criminal procedure rules on investigation of alleged offences, and admissibility of data as evidence. Not all States have the expertise and rules necessary for successful investigation and prosecution and even where they exist, ensuring these bodies have the capacity to absorb and keep up with rapidly changing technology presents a further challenge.

The CRC Committee highlights the particular challenges faced by children in accessing justice for violations of their rights in connection with the digital environment. These challenges include the lack of legislation imposing appropriate sanctions for violations of children's rights in the digital environment and challenges obtaining the necessary digital evidence and identification of the perpetrator to initiate a prosecution.²³ Further, children, parents and legal guardians may not have sufficient knowledge or awareness of their rights in the digital environment to claim them. Even where such knowledge and awareness exist, children and/or their families may be reluctant to report violations due to the sensitivity of the subject and fears of reprisals or of social exclusion.²⁴

Child victims may experience continuing trauma where child sexual abuse material circulates online, often for long periods of time. This reinforces the need for procedures to be put in place for the taking down of such material, involving a range of stakeholders including law enforcement, regulators, civil society and industry stakeholders.

Year on year, there are increasing reports of various forms of online child sexual exploitation and abuse. The reported increase in the scale, severity and complexity of online child sexual abuse and exploitation, particularly during the Covid-19 pandemic, is of particular concern.²⁵ For example, in 2021, the US-based National Center for Missing and Exploited Children received 29.3 million reports of suspected child sexual exploitation, an increase of 35 per cent from 2020.²⁶ Concerningly, the true extent of the problem is unknown, in part due to barriers to disclosure and reporting of child sexual exploitation and abuse.

For some time, research on the extent of online child sexual abuse and exploitation related mostly to high-income countries. However, there is increasing research from low and middle-income countries on the issue. Interviews with children across 12 countries in the East Asia and Pacific and Eastern and Southern Africa regions during 2020-2021 indicated that between one to 20 per cent of children suffered online sexual exploitation and abuse in the past year, one in three of whom did not tell anyone about this experience.²⁷

Reports indicate that identification of, and provision of support to, victims of online child sexual exploitation and abuse have not kept pace with the increase in the numbers of reported cases. This lag is due, in part, to limited access by law enforcement to the technology and the set-up needed to identify and follow-up cases,²⁸ and lack of sufficient services available to provide the necessary psychological and other forms of support to child victims.

1.3 Duty of States to protect children from online child sexual exploitation and abuse

Online child sexual exploitation and abuse is a violation of children's rights, particularly the right of the child to protection from all forms of sexual exploitation and abuse. Article 34 of the CRC places a clear obligation on States parties to take action to protect children from these violations.

The OPSC elaborates on States parties' obligations to combat particular forms of child sexual exploitation and abuse, namely '*child prostitution*', '*child pornography*' (more appropriately referred to as child sexual abuse materials) and the sale of children.



Article 34 of the CRC

'States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:

- (a) The inducement or coercion of a child to engage in any unlawful sexual activity;
- (b) The exploitative use of children in prostitution or other unlawful sexual practices;
- (c) The exploitative use of children in pornographic performances and materials.'



It is generally accepted under international standards that the term '*child pornography*' should be avoided to the extent possible and replaced by terms such as '*child sexual abuse material*',²⁹ as the term '*pornography*' does not appropriately reflect the abusive aspect of the issue and risks undermining its severity.³⁰

Although the CRC and OPSC do not expressly refer to '*online*' child sexual exploitation and abuse, the CRC Committee's General Comment No. 25 (2021) on children's rights in relation to the digital environment affirms the obligation of States parties

to protect children from all forms of violence in the digital environment, including through legislative measures.

*'States parties should take legislative and administrative measures to protect children from violence in the digital environment, including the regular review, updating and enforcement of robust legislative, regulatory and institutional frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment. Such risks include... **exploitation and abuse, including sexual exploitation and abuse**..... States parties should implement safety and protective measures in accordance with children's evolving capacities.'*³¹ (Emphasis added)

The CRC Committee has published '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' (OPSC Guidelines). The OPSC Guidelines confirm the application of the OPSC to the sale of children, child prostitution and child

pornography with links to the digital environment and recommend that States parties should prevent and address online sexual exploitation and abuse of children through their measures to implement the OPSC.³²

*'States parties should prevent and address online sale, sexual exploitation and sexual abuse of children through their implementation measures. National legal and policy frameworks should be assessed to ensure that they adequately cover all manifestations of the sale, sexual exploitation and sexual abuse of children, including when these offences are committed or facilitated through ICT.'*³³

The increase in online child sexual abuse and exploitation and calls from country-level stakeholders for practical guidance have reinforced the urgent need to elaborate the minimum and recommended standards that should be incorporated into legislation to protect children from such violence. It is against this backdrop that this Global Guide was developed.

1.4 Development of the Global Guide

The Global Guide is based on international conventions, regional conventions, guidelines and model laws as well as the views of UN bodies, national governments, international experts, civil society and business representatives from across the world. The key instruments are listed here and are referred to in the text.

Key international conventions³⁴

- United Nations Convention on the Rights of the Child;³⁵
- Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography;³⁶
- International Labour Organization Convention 1999 No. 182 on the Worst Forms of Child Labour;³⁷
- Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (Palermo Protocol).³⁸

Key regional standards

- African Charter on the Rights and Welfare of the Child;³⁹
- African Union Convention on Cyber Security and Personal Data Protection;⁴⁰
- Arab Convention on Combating Information Technology Offences;⁴¹
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual

Abuse (Lanzarote Convention), which is also open to accession by non-Council of Europe States;⁴²

- Council of Europe Convention on Cybercrime (Budapest Convention) and its Protocols, which are also open to accession by non-Council of Europe States;⁴³
- Declaration on the Protection of Children from All Forms of Online Exploitation and Abuse in the Association of Southeast Asian Nations (ASEAN);⁴⁴
- Economic Community of West African States' Directive C/DIR 1/08/11 on Fighting Cyber Crime;⁴⁵
- EU Directive 2011/93 of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography;⁴⁶
- EU Directive 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Directive 2016/680/EU).⁴⁷

General Comments of the Committee on the Rights of the Child and the African Committee of Experts on the Rights and Welfare of the Child

- The general comments of the Committee on the Rights of the Child, including:
 - General Comment No. 25 (2021) on children's rights in relation to the digital environment;⁴⁸
 - General Comment No. 24 (2019) on children's rights in the child justice system;⁴⁹ and
 - General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights;⁵⁰
- African Committee of Experts on the Rights and Welfare of the Child's General Comment No. 7 (2021) on Article 27 of the African Charter on the Rights and Welfare of the Child;⁵¹
- 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.⁵²

Key guidelines and model laws

- Caribbean Community, Model Policy Guidelines and Legislative Texts on Cybercrime/e-Crime;⁵³
- Council of Europe, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment;⁵⁴
- International Centre for Missing and Exploited Children, Model Legislation on Combatting Grooming of Children for Sexual Purposes;⁵⁵
- International Centre for Missing and Exploited Children, Model Legislation on Child Sexual Abuse Material;⁵⁶
- Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN 2021-2025;⁵⁷
- Southern African Development Community Model Law on Computer Crime and Cybercrime;⁵⁸
- Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, also known as the 'Luxembourg Guidelines';⁵⁹
- WeProtect Global Alliance's Model National Response Framework and the Global Strategic Response (2016).⁶⁰



This Guide also draws on examples of legislative drafting from a range of countries. While the authors have endeavored to verify the contemporaneity and accuracy of the Laws and Bills when developing and finalizing the Global Guide, it is possible that these texts have undergone amendments which are not reflected in the Global Guide.



The international and regional conventions, guidelines and model laws have different legal authority under international law. Conventions create binding obligations for States parties while ‘*soft law*’ standards such as guidelines and principles, though not legally binding, can provide authoritative interpretations of treaty obligations or reflect binding customary international law. To reflect these varying levels of legal authority, this Global Guide adopts the following approach:

- For obligations under international conventions which States have ratified, most notably the CRC, the Global Guide recommends that States ‘**ensure**’ the incorporation of the standard in their national legal frameworks.
- For regional conventions, which some States have ratified, and general comments and guidelines of treaty bodies, most notably the CRC Committee, the Global Guide recommends that States ‘**should**’ incorporate the standard into their national legal frameworks.
- For other international and regional guidelines or principles and model laws, which are not necessarily explicitly mentioned in international or regional conventions or soft law standards but are regarded as good practice or are an emerging practice, the Global Guide recommends that States ‘**consider**’ the incorporation of the standard into their national legal frameworks.

In any event, stakeholders should familiarize themselves with relevant international and regional conventions to which their State is a party, as these create binding international legal obligations on their State. It is noted, however, that international and regional conventions contain the minimum standards for the protection of human rights, including children’s rights. States may therefore consider integrating higher standards for the protection of human rights which go beyond their minimum obligations under international and regional conventions.⁶¹

The digital environment is also constantly evolving, raising new and emerging opportunities and risks for the protection of human rights, including children’s rights. International and regional standards are likely to evolve over time to reflect these developments. Therefore, consideration should be made to any amendments to international and regional conventions, general comments and guidelines and model laws introduced after the date of this Global Guide and their implications for domestic legal reform.

Refer to this colour coding in the checklist on **page 24** to understand the varying levels of authority

1.5 Structure of the Global Guide

This Global Guide is divided into 12 key parts, each of which contains guidance on a particular thematic area or aspect of legislative reform. The 12 parts are as follows:

1. Introduction	A brief introduction to the purpose of and context behind this Global Guide. This part defines the key terms used in the Guide, as well as a list of the key international and regional conventions, general comments and guidelines of treaty bodies and model laws on which this Global Guide is based.
2. Consolidated checklist	This part contains a consolidated checklist of the minimum and recommended standards for legislative reform set out in this Global Guide.
3. Evidence-based legislation	This part provides guidance on the need to ensure that the State has high quality data on the trends and prevalence of child sexual exploitation and abuse to assist it in drafting legislation that focuses on children's lived experiences and the 'harms' caused by online sexual exploitation and abuse. This part also provides examples of good practice which States can draw on including mechanisms for integrating the views of children in the development of legislation.
4. Stakeholder engagement and catalysts for legal reform	This part provides guidance on the legislative reform process, including potential entry points, techniques for engaging legislators, policymakers and other key stakeholders.
5. Methods of legislative reform	This part provides guidance on identifying methods of legislative reform and the framework within which new legislation can be introduced. Considerations include whether legislative reform should take place by amending existing legislation, or introducing a new law, or a combination of these approaches, and whether provisions concerning online child sexual exploitation and abuse should be included in a child rights law, cybersecurity law, criminal code or other type of legislation.
6. Criminalization of online child sexual exploitation and abuse	This part provides guidance and concrete examples on the different types of online child sexual exploitation and abuse that should be criminalized. It also sets out guidance from authoritative sources on dealing with complex, new or emerging issues that may arise during the legislative drafting process, including the handling of cases involving self-generated sexual material by children, or cases involving consensual acts between peers who are close in age and psychological and physical development and maturity.
7. Duties and responsibilities in relation to business	This part provides guidance on approaching the duties and responsibilities of businesses and the private sector in protecting children from online child sexual exploitation and abuse and the minimum and recommended standards for inclusion in the legislation which establishes this framework.
8. Procedures and methods of investigation of online child sexual exploitation and abuse	This part provides essential background information on the procedures and mechanics of investigating and prosecuting online child sexual abuse and exploitation by law enforcement bodies, and the minimum standards for inclusion in primary legislation in order to implement the procedures in practice.

9. Victim support, rehabilitation, reintegration and redress	This part focuses on the minimum and recommended standards to ensure the protection of the rights of victims of online child sexual exploitation and abuse. It includes standards on providing adequate redress as well as the provision of support, rehabilitation and reintegration services.
10. Independent monitoring and regulation	This part outlines the important role that national human rights institutions and independent regulation play in protecting and promoting children’s right to protection from online sexual exploitation and abuse and minimum and recommended standards and considerations for inclusion in legislation.
11. Implementation of legislation	This part provides an overview of other key elements, besides legislative reform, that should be put in place in order to prevent and respond to online child sexual exploitation and abuse and ensure the effective implementation of legislation on this topic.
12. Glossary	This part provides descriptions of the technical terms used throughout the Global Guide.

1.6 Definitions and terminology

A potential challenge with drafting legislation on online child sexual exploitation and abuse is defining the acts which fall within its scope and agreeing on a universally accepted terminology. The CRC Committee has recognized that terms used in international treaties and optional protocols, such as the use of the term ‘*child pornography*’ in the OPSC, are gradually being replaced.⁶² The CRC Committee therefore encourages States parties and other relevant stakeholders ‘*to pay attention*’ to the Luxembourg Guidelines regarding the terminology to be used in laws and policies to combat the sexual exploitation and abuse of children.⁶³

The Luxembourg Guidelines provide some clarity and interagency consensus on the use of terms relating to child sexual exploitation and abuse, however, they do not reflect a global consensus of these terms.⁶⁴ In addition, the Luxembourg Guidelines mostly provide general descriptions rather than ‘*legal*’ definitions that can be adopted

in legislation, and do not necessarily capture the new or emerging means of online child sexual exploitation and abuse or terminology.

When drafting definitions of online child sexual exploitation and abuse, it is important to ensure that the terms are ‘where possible formulated in a technology-neutral manner, leaving room for the emergence of new technologies’.

The Council of Europe’s Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment also address the challenges of defining online child exploitation and abuse and recommend that when drafting definitions of online child sexual exploitation and abuse, it is important to ensure that the terms are ‘*where possible formulated in a technology-neutral manner, leaving room for the emergence of new technologies*’.⁶⁵

For the purposes of this Global Guide, the terms used are defined as follows:

Child	A person under the age of 18 years. ⁶⁶
Child sexual abuse	The involvement of a child in sexual activity that they do not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent. ⁶⁷ Child sexual abuse does not necessarily involve physical contact and can take the form of non-contact abuse. ⁶⁸
Child sexual abuse material	Any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child for primarily sexual purposes ⁶⁹ , including live-streaming. As recommended by the CRC Committee and in the Luxembourg Guidelines, the term ‘ <i>child pornography</i> ’ should be avoided to the extent possible and replaced by terms such as ‘ <i>child sexual abuse material</i> ’ ⁷⁰ , which is the approach taken in this Global Guide. The main reason for this approach is that the term ‘ <i>pornography</i> ’ does not appropriately reflect the abusive aspect of the issue and risks undermining its severity. ⁷¹

<p>Child sexual exploitation</p>	<p>This occurs when a child takes part in a sexual activity in exchange for something (e.g. gain or benefit, or even the promise of such) from a third party or the perpetrator. A child may be coerced into a situation of sexual exploitation through physical force or threats or be persuaded to engage in the sexual activity as a result of human or situational factors, such as a power imbalance between the victim and the perpetrator.⁷²</p>
<p>Child victim</p>	<p>A child who has been subjected to or experienced online child sexual exploitation and abuse.</p> <p>In accordance with the Luxembourg Guidelines, this terminology does not take into account how the child feels about their situation and is not intended to label the child. Rather, it is used to reflect the fact that the child has experienced or been subjected to online child sexual exploitation and abuse. Further, in the context of legislative drafting, particularly police investigations and judicial proceedings, this term is necessary in order for the child to be recognized by law as eligible for redress and to clarify that the child is not responsible and should not be blamed for the violence.⁷³ It is for these reasons why the Global Guide adopts the term ‘<i>victim</i>’ instead of ‘<i>survivor</i>’.</p>
<p>Digital environment / online</p>	<p>This encompasses ‘<i>information and communications technologies, including digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology</i>’.⁷⁴</p>
<p>Information and communication technology or ‘ICT’ / digital technologies</p>	<p>A ‘<i>diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.)</i>’.⁷⁵</p>
<p>Legislation</p>	<p>Legislation refers to primary legislation and secondary legislation. Primary legislation refers to legislation that is passed by the full legislative body of the State, usually in the form of a Law, a Code or an Act. Secondary legislation refers to delegated or subsidiary legislation usually passed by a minister or other competent body given power under the primary legislation. It generally takes the form of regulations, rules, directives or statutory guidance or guidelines.</p>
<p>Online child sexual abuse</p>	<p>The term online sexual abuse of children is widely used to refer both to sexual abuse of children that is facilitated by ICTs (for example, online grooming) and to sexual abuse of children that is committed elsewhere and then repeated by sharing it online. This latter scenario occurs where, for instance, a child is sexually abused offline but photos or videos of the abuse (constituting child sexual abuse material) are then uploaded, distributed and accessed online.⁷⁶</p>

<p>Online child sexual exploitation</p>	<p>The sexual exploitation of children facilitated by the use of ICTs.⁷⁷ It includes <i>‘all acts of a sexually exploitative nature carried out against a child that have at some stage, a connection to the online environment’</i>.⁷⁸ It includes:</p> <ul style="list-style-type: none"> • Any <i>‘use of ICT that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted’</i>;⁷⁹ • Sexual exploitation that is carried out while the victim is online (such as enticing/manipulating/threatening a child into performing sexual acts in front of a webcam);⁸⁰ • Identifying and/or grooming potential child victims online with a view to exploiting them sexually, whether or not the acts that follow are carried out online;⁸¹ • The distribution, dissemination, importing, exporting, offering, selling, possession of, or knowingly obtaining access to child sexual exploitation material online, even if the sexual abuse that is depicted in the material was carried out offline.⁸²
<p>Virtual child sexual abuse</p>	<p>This is a term sometimes used as a synonym for <i>‘online child sexual abuse’</i>. However, care should be taken not to confuse these two terms, which have very different meanings. <i>‘Virtual’</i> relates to online artificially or digitally created images of children involved in sexual activities. The realism of such images creates the illusion that children are actually involved, although this is not the case.⁸³ However, it is also noted that such depictions of children are also being described as <i>‘digitally created or altered’</i> rather than <i>‘virtual’</i>. With the move into the metaverse and other virtual reality immersive technology, the understanding of <i>‘virtual child abuse’</i> may be more focused on where there is an actual child end-user who is subject to abuse in a virtual environment.</p>

Part 12: Glossary provides descriptions of other technical terms used throughout the Global Guide.

Endnotes

- 11 Committee on the Rights of the Child (CRC Committee), General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021 (CRC General Comment No. 25 (2021)). The CRC Committee includes information and communications technologies, digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology within its understanding of the term 'digital environment'.
- 12 United Nations Children's Fund, Request for Proposal for Services: Improving legislative frameworks to protect children from online child sexual exploitation and abuse, 2021, p. 1; UNICEF et al., COVID-19 and its implications for protecting children online, April 2020; CRC General Comment No. 25 (2021), para. 80.
- 13 CRC General Comment No. 25 (2021), para. 3.
- 14 Ibid, para. 80.
- 15 Luxembourg Guidelines, p. 28.
- 16 UNICEF, Ending Online Child Sexual Exploitation and Abuse: Lessons learned and promising practices in low and middle income countries, UNICEF, New York, December 2021, p. 10.
- 17 ICMEC, Child Sexual Abuse Material: Model Legislation and Global Review, 9th Edition, 2018, p. 1.
- 18 International Centre for Missing and Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 2017.
- 19 ICMEC, Child Sexual Abuse Material: Model Legislation and Global Review, 9th Edition, 2018, p. 1.
- 20 International Centre for Missing and Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 2017.
- 21 Ibid.
- 22 UNICEF Latin America and Caribbean Regional Office and ICMEC, Online Child Sexual Abuse and Exploitation, Guidelines for the Adoption of National Legislation in Latin America, 2016, p. 4.
- 23 CRC General Comment No. 25 (2021), para. 43.
- 24 Ibid.
- 25 EUROPOL, Covid-19 Sparks Upward Trend in Cybercrime, Press Release, 5 October 2020, <www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime>, accessed 28 September 2021; INTERPOL, Threats and Trends: Child Sexual Exploitation and Abuse – Covid Impact, September 2020.
- 26 National Center for Missing and Exploited Children, CyberTipline 2021 Report, <www.missingkids.org/gethelpnow/cybertipline/cybertipline-data>, accessed 10 May 2022.
- 27 United Nations Children's Fund (UNICEF) Office of Research - Innocenti, Children's experiences of online child sexual exploitation and abuse in 12 countries in Eastern and Southern Africa and Southeast Asia, Disrupting Harm Data Insights, Global Partnership to End Violence Against Children (forthcoming).
- 28 Professor Michael Salter et al., Research Report: The Impact of Covid-19 on the Risk of Online Child Sexual Exploitation and the Implications for Child Protection and Policing, UNSW Sydney, May 2021, pp. 16, 29 and 36.
- 29 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 (OPSC Guidelines), CRC/C/156, 10 September 2019, para. 60; Luxembourg Guidelines, pp 37-38.
- 30 Luxembourg Guidelines, p 38.
- 31 CRC General Comment No. 25 (2021), para. 82.
- 32 OPSC Guidelines, paras. 9(c) and 37.
- 33 Ibid, para. 37.
- 34 At the time of writing this report, UN Member States have begun negotiating a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes in accordance with General Assembly resolution 75/282 and with General Assembly decision 76/552. While the offences to be included are yet to be determined, a number of Member States have submitted that online child sexual exploitation and abuse should be included. The proposed scope of the convention is detailed here: <www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/V2201067.pdf>, accessed 15 March 2022.
- 35 Convention on the Rights of the Child, <https://downloads.unicef.org.uk/wp-content/uploads/2010/05/UNCRC_united_nations_convention_on_the_rights_of_the_child.pdf>
- 36 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, <<https://www.ohchr.org/sites/default/files/crc-sale.pdf>>, accessed 10 May 2022.
- 37 International Labour Organization (ILO) Convention 1999 No. 182 on the Worst Forms of Child Labour, <www.ilo.org/wcmsp5/groups/public/-/ed_norm/-/declaration/documents/publication/wcms_decl_fs_46_en.pdf>, accessed 10 May 2022.
- 38 Palermo Protocol, <www.ohchr.org/sites/default/files/ProtocolonTrafficking.pdf>, accessed 10 May 2022.
- 39 African Charter on the Rights and Welfare of the Child, <https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf>, accessed 10 May 2022.
- 40 African Union Convention on Cyber Security and Personal Data Protection, <www.au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf>, accessed 15 March 2022.
- 41 Arab Convention on Combating Information Technology Offences, <www.asianlaws.org/gclid/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf>, accessed 15 March 2022.
- 42 Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), 25 October 2007, <<https://rm.coe.int/1680084822>>, accessed 15 March 2022.
- 43 Council of Europe, Convention on Cybercrime (ETS No. 185), 23 November 2001, <<https://rm.coe.int/1680081561>>, accessed 15 March 2022; Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No.189), 28 January 2003, <<https://rm.coe.int/168008160f>>, accessed 15 March 2022; Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 17 November 2021, <<https://rm.coe.int/1680a49dab>>, accessed 15 March 2022.
- 44 Declaration on the Protection of Children from All Forms of Online Exploitation and Abuse in the Association of Southeast Asian Nations (ASEAN), <<https://asean.org/wp-content/uploads/2019/11/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf>>, accessed 10 May 2022.
- 45 Economic Community of West African States, Directive C/DIR 1/08/11 on Fighting Cyber Crime, <www.issafrica.org/ctafrika/uploads/Directive%201-08-11%20on%20Fighting%20Cyber%20Crime%20with-in%20ECOWAS.pdf>, accessed 10 May 2022.
- 46 EU Directive 2011/93, <<https://op.europa.eu/en/publication-detail/-/publication/d20901a4-66cd-439e-b15e-faeb92811424/language-en>>, accessed 15 March 2022.
- 47 EU Directive 2016/680, <<https://eur-lex.europa.eu/legal-content/EN/TX/?uri=CELEX%3A02016L0680-20160504>>, accessed 24 May 2022.
- 48 CRC General Comment No. 25 (2021), <<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>>, accessed 10 May 2022.

- 49 CRC Committee, General Comment No. 24 (2019) on children's rights in the child justice system, CRC/C/GC/24, 18 September 2019, <<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-24-2019-childrens-rights-child>>, accessed 10 May 2022.
- 50 CRC Committee, General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16, 17 April 2013 (CRC General Comment No. 16 (2013)), https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f16&Lang=en, accessed 10 May 2022.
- 51 General Comment No. 7 (2021) on Article 27 of the African Charter on the Rights and Welfare of the Child, https://www.acerwc.africa/wp-content/uploads/2021/09/General-Comment-on-Article-27-of-the-ACRWC_English-1.pdf, accessed 10 May 2022.
- 52 OPSC Guidelines, CRC/C/156, 10 September 2019, www.ohchr.org/sites/default/files/Documents/HRBodies/CRC/CRC.C.156_OPSC_Guidelines.pdf, accessed 10 May 2022.
- 53 Group of African, Caribbean and Pacific States and others, Model Policy Guidelines and Legislative Texts, p. 12, <www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cyber-crimes.pdf>, accessed 10 November 2021.
- 54 Council of Europe, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, September 2018, <<https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>>, accessed 15 March 2022.
- 55 International Centre for Missing and Exploited Children, Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 1st Edition, 2017, <www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf>, accessed 5 January 2022.
- 56 International Centre for Missing and Exploited Children, Child Sexual Abuse Material: Model Legislation and Global Review, 9th Edition, 2018, <<https://cdn.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18-1.pdf>>, accessed 5 January 2022.
- 57 ASEAN, Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN (2021-2025), October 2021, https://asean.org/wp-content/uploads/2021/11/4.-ASEAN-RPA-on-COEA_Final.pdf, accessed 10 May 2022.
- 58 Southern African Development Community Model Law on Computer Crime and Cyber Crime, <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf>, accessed 10 May 2022.
- 59 Luxembourg Guidelines, www.ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf, accessed 5 January 2022.
- 60 WeProtect Global Alliance, Frameworks, <https://www.weprotect.org/frameworks/>, accessed 10 May 2022.
- 61 For example, Article 41 of the CRC provides that, 'Nothing in the present Convention shall affect any provisions which are more conducive to the realization of the rights of the child and which may be contained in: (a) The law of a State party; or (b) International law in force for that State.'
- 62 CRC Committee, 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, 10 September 2019 (OPSC Guidelines), para. 5.
- 63 OPSC Guidelines, para. 5.
- 64 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, (the Luxembourg Guidelines), p. 16.
- 65 Council of Europe Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, para. 74, <<https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html>>, accessed 15 February 2022.
- 66 The general rule in the Convention on the Rights of the Child (CRC), Art. 1; African Charter on the Rights and Welfare of the Child (ACRWC), Art. 2; ILO Convention No. 182, Art. 2; Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, (the Luxembourg Guidelines) A3, p. 6.
- 67 WeProtect Global Alliance, Global Threat Assessment 2021, p. 10.
- 68 Luxembourg Guidelines, C3, pp. 19-20.
- 69 OPSC, Article 2.
- 70 OPSC Guidelines, para 60. See also Luxembourg Guidelines, pp 37-38.
- 71 Luxembourg Guidelines, p 38.
- 72 Ibid., D3, pp. 24-25
- 73 Ibid., pp. 77-78.
- 74 CRC General Comment No. 25 (2021), para. 2.
- 75 United Nations Educational, Scientific and Cultural Organization, Institute for Statistics, Information and Communications Technologies (ICT), <http://uis.unesco.org/en/glossary>, accessed 24 May 2022.
- 76 The Luxembourg Guidelines, C.4.vi, p. 23.
- 77 Ibid., p. 27.
- 78 Ibid., p. 27.
- 79 Ibid., p. 27.
- 80 Ibid., p. 27.
- 81 Ibid., p. 28.
- 82 Ibid., p. 28.
- 83 Ibid., C.4.vi, p. 23.



See the key on **page 15** for an explanation of the colour coding

2. Consolidated checklist

2.1 Evidence-based legislation

High quality and disaggregated data on all forms of child sexual exploitation and abuse **should** be collected.

Ensure data on the trends and prevalence of online child sexual exploitation and abuse informs the development of primary and secondary legislation.

Ensure children and young people's views are considered as a key element of the development of legislation related to online child sexual exploitation and abuse.

Civil society expertise, including from NGOs, industry and academia, **should** be involved in the development of legislation related to online child sexual exploitation and abuse.

Multi-sector monitoring bodies **should** share information and inform the development of policy and practice.

Existing legislation **should** be monitored and evaluated to ensure it complies with international and regional standards and best practice.

2.2 Stakeholder engagement and catalysts for legal reform

Advocacy and other communications strategies **should** raise awareness of child sexual exploitation and abuse including forms facilitated by the use of information and communication technologies, based on up-to-date research and information

Links to broader and/or related initiatives concerning the protection of children, such as movements to address violence against women and/or children, or broader cybersecurity or digitalisation initiatives, **should** be identified and used as entry points for stakeholder engagement and legislative reform

Collaboration with key strategic stakeholders within government **should** be strengthened in order for government to take the lead in the development of policy and legislative reforms

Consider leveraging the influence and leadership of regional and international inter-governmental organizations to promote national legal reforms

2.3 Methods of legislative reform

The method of legislative reform (amending an existing law, developing a new law or a combination of both) and the thematic framework (criminal code, cybercrime, child protection, online safety, and/or other) in which to introduce the reforms **should** be identified

Consequential amendments to other laws **should** be identified

2.4 Criminalization of online child sexual exploitation and abuse

Ensure that a child is defined as any person under the age of 18 years

Ensure the inclusion of a comprehensive definition of sexual abuse and exploitation of children, including where it is facilitated with the use of ICTs

Ensure that presumed consent by the child to the abuse or exploitation is null and void

Adolescents who are close in age, maturity and development **should not** be criminalized for consensual and non-exploitative sexual activity, provided that there is no element of coercion, abuse of trust or dependency between the adolescents, regardless of whether or not it is facilitated by the use of ICTs

Ensure that the law includes specific crimes relating to producing, offering, distributing, disseminating, importing, exporting, interacting with, accessing, possessing, and producing or disseminating material to advertise, child sexual abuse material, including live-streaming of child sexual abuse

A child **should not** be held criminally liable for the generation, possession, or voluntary and consensual sharing of sexual content of him/herself, solely for own private use, but instead States **should**:

- Establish clear legal frameworks that protect children and
- Through prevention efforts, ensure that children are educated about and made aware of the gravity of spreading content of others and of oneself

Sexual extortion of children **should** be criminalized, regardless of whether or not it is facilitated by the use of ICTs

Grooming of children **should** be criminalized, regardless of whether or not it is facilitated by the use of ICTs

Ensure the criminalization of attempts, complicity and participation in offences contained within the OPSC and consider criminalizing attempts, complicity and participation in other online child sexual exploitation and abuse offences

Consider including a specific offence of intentionally causing a child, for sexual purposes, to witness sexual abuse or sexual activities through the use of ICTs, including where the child is not required to participate (subject to the standards above on self-generated sexual content)

Consider including other specific crimes relating to online child sexual exploitation and abuse, such as 'cyberflashing' or 'cyberstalking'

Consider introducing universal jurisdiction for all offences of child sexual exploitation and abuse, irrespective of whether or not they are facilitated with the use of information and communication technologies, and removing any requirement for 'double criminality' for such offences

Child sexual exploitation and abuse offences **should** be recognized by law as extraditable offences, regardless of whether or not they are facilitated by the use of information and communication technologies

Extradition **should not** be conditional upon the existence of an extradition treaty with the other concerned State(s)

Law enforcement authorities **should** be required to take suitable measures to submit the case to its competent authorities for the purpose of prosecution in the event that the alleged perpetrator is not extradited on the basis of the alleged perpetrator's nationality

The statute of limitations in respect of offences of child sexual exploitation and abuse, irrespective of whether or not it is facilitated by the use of information and communication technologies, **should** be removed

Ensure minimum penalties/sanctions for adult perpetrators and enhanced penalties/sanctions for aggravating factors including young age of the victim

Ensure that children alleged as, accused or convicted of a crime, including of online child sexual exploitation and abuse offences, are handled within a separate child justice system in accordance with child-friendly justice principles and procedures

2.5 Duties and responsibilities in relation to business

Duties and responsibilities of businesses **should** be approached using a rights-based approach, within the broader framework of the UN Guiding Principles on Business and Human Rights

Legislation to regulate businesses conduct, services and design of digital technologies **should** place children's rights at the core

Consider requiring businesses to adopt age assurance mechanisms, consistent with data protection and safeguarding requirements, to prevent children's access or exposure to pornography and other illegal or age-restricted sexual content

Consider introducing requirements for businesses to establish 'notice and takedown' procedures, including a requirement to block or remove child sexual abuse material notified to it by a trusted flagger recognized by law

Consider introducing provisions into relevant laws to enable businesses to detect proactively child sexual abuse material accessed or stored on their products and services for the purpose of blocking or removing such materials, provided that the law requires such measures to be legal, necessary and proportionate and the least intrusive option available, without impairing the essence of the individual's right to privacy

Consider making it mandatory for businesses to report online child sexual abuse material to law enforcement or other designated reporting body

Ensure the availability of a range of criminal, civil and administrative sanctions for legal persons for offences relating to online child sexual exploitation and abuse and violations of obligations to protect children from such harms

2.6 Procedures and methods of investigation of online child sexual exploitation and abuse

A point of contact **should** be designated in the legislation to receive referrals, leads and tips regarding suspected cases and to provide immediate assistance for the purpose of investigations or proceedings concerning online child sexual exploitation and abuse offences

A national specialized unit **should** be established with an explicit mandate to lead, support and coordinate investigations as well as specialist law enforcement investigation units at sub-national level dedicated to investigating online child sexual exploitation and abuse

Consider introducing a legal requirement for staff to have minimum qualifications and complete pre-service and regular in-service training before working on child protection and child sexual exploitation cases, the details of which may be elaborated in secondary legislation or determined by the relevant professional regulatory authority or training authority

Legislation **should** establish the powers and procedures for undertaking criminal investigations of online child sexual exploitation and abuse

Undercover investigations **should** be permitted but regulated by law and comply with international human rights standards

Ensure that it is possible to convict an alleged perpetrator of attempting to commit a child sexual exploitation and abuse offence, even where in fact it would have been impossible for the full offence to have been committed (to cover cases where undercover law enforcement pretends to be a child, another offender ('customer') or co-conspirator)

Legislation **should** allow law enforcement to 'triage' cases once reported

Ensure that legislation contains powers for law enforcement to enter a building and seize/remove stored computer data

Ensure that child victims found during search and seizure operations fall within the scope of child protection laws and are referred to the designated child protection authority

Standard operating procedures and inter-agency joint working protocols **should** be put in place to ensure effective coordination between law enforcement, child protection authority and other relevant agencies in safeguarding the child

Consider developing standard operating procedures for the police to assist investigators on the policies and procedures to be followed when undertaking search and seizure to ensure the admissibility of evidence in a court of law

Legislation **should** be adopted to enable competent authorities to order or obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, particularly where there are grounds to believe that the computer data is particularly vulnerable to loss or modification

Legislation **should** set out provisions relating to the 'chain of custody' of digital data and devices to maintain the integrity of evidence

Consider making formal arrangements to access secure international (and particularly Interpol) image databases and/or developing a national database

Legislation **should** set out rules on the admissibility of digital and forensic evidence

State law enforcement and criminal investigation and prosecution authorities in the State **should** cooperate and provide mutual legal assistance to equivalent bodies in other States to the widest extent possible for the purposes of investigating and prosecuting online sexual exploitation and abuse of children, including with regard to obtaining evidence, and to identifying and protecting child victims

Ensure that mutual legal assistance with another State is not conditional on the existence of a treaty for mutual legal assistance with that State

2.7 Victim support, rehabilitation, reintegration and redress

Ensure child friendly practices and support are applied to child victims and witnesses in the justice system

Rehabilitation and reintegration services **should** be strengthened to address the unique needs of child victims of online sexual abuse and exploitation

Services to prevent further victimization **should** be available to child victims and their families

Ensure specialist training on the digital context is provided to the workforce that responds to child victims of sexual abuse and exploitation

Collaboration and coordination between the different stakeholders involved in child sexual exploitation cases and child protection services **should** be formalized

Measures that ensure sufficient financial resources are allocated annually to victim support services **should** be introduced

Consider establishing a helpline that provides detailed information and referrals to the relevant service provider

Consider establishing clear procedures for the swift removal of child sexual abuse materials

Differing forms of and platforms for compensation **should** be offered to child victims

2.8 Independent monitoring and regulation

Ensure that children's rights in relation to the digital environment, including their rights to protection, are integrated into the legislative mandate and activities of the State's national human rights institution (NHRI) for children

Children's online protection **should** be integrated within the mandate of independent regulatory systems for the digital environment, which should work in collaboration with other monitoring bodies, particularly the NHRI, to protect children from online child sexual exploitation and abuse

Consider the establishment of an independent regulator for online safety, including the protection of children from online sexual exploitation and abuse

2.9 Implementation of legislation

Secondary legislation, including Standard Operating Procedures and Guidelines, and other authoritative guidance to give effect to primary legislation **should** be developed to combat online child sexual abuse and exploitation

Ensure children are educated on their rights and responsibilities in the digital environment, including on the risks of online sexual exploitation and abuse, safe online practices and available support and reporting mechanisms

Ensure parents and caregivers are educated on the digital environment, including its benefits, the risks of online sexual exploitation and abuse, safe online practices and available support and reporting mechanisms

Professionals who work with and for children **should** receive training on the identification of children at risk, support services and reporting mechanisms, and opportunities and risks in relation to the digital environment, including different forms of technology

Law enforcement professionals **should** receive training in best practice that is contextualized to the countries' legal framework for the effective investigation and prosecution of online offences

Ensure sufficient financial and human resources are allocated annually to give effect to legislation designed to combat online child sexual abuse and exploitation

3. Evidence-based legislation

Checklist of minimum and recommended standards

High quality and disaggregated data on all forms of child sexual exploitation and abuse **should** be collected

Ensure data on the trends and prevalence of online child sexual exploitation and abuse informs the development of primary and secondary legislation

Ensure children and young people's views are considered as a key element of the development of legislation related to online child sexual exploitation and abuse

Civil society expertise, including from NGOs, industry and academia, **should** be involved in the development of legislation related to online child sexual exploitation and abuse

Multi-sector monitoring bodies **should** share information and inform the development of policy and practice

Existing legislation **should** be monitored and evaluated to ensure it complies with international and regional standards and best practice

The CRC Committee's General Comment No. 25 (2021) requires that all States parties to the CRC should 'review, adopt and update national legislation in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention and the Optional Protocols'.⁸⁴ Before doing so, however, the CRC Committee recommends that States parties collect 'robust, comprehensive, disaggregated data that is adequately resourced and that data are disaggregated by age, sex, disability, geographical location, ethnic and national origin, and socioeconomic background. Such data and research, including research conducted with and by children,

should inform legislation, policy and practice and should be available in the public domain'.⁸⁵

Laws and guidelines at the regional level also affirm the need for evidence-based legislation to combat online sexual abuse and exploitation. Similar to the recommendations of the CRC Committee, the African Committee of Experts on the Rights and Welfare of the Child (ACRWC Committee) interprets Article 27 of the African Charter on the Rights and Welfare of the Child (ACRWC) to mean that 'legal and policy frameworks should be reviewed and where necessary adapted to rapidly changing realities concomitant with developments in the digital world'.⁸⁶

3.1 Detail of minimum and recommended standards

High quality and disaggregated data on all forms of child sexual exploitation and abuse **should** be collected

The OPSC Guidelines⁸⁷ recommend that data should be collected on the *'number of cases reported, prosecutions, convictions and sanctions, preferably including redress provided to victims, disaggregated by the nature of the offence including with regard to online and offline activity, the category of perpetrator and the relationship between the perpetrator and the victim, and the sex and age of the child victim'*.⁸⁸

Collection of data and monitoring are also key elements of the WeProtect Model National Response. The non-binding Model National Response recommends that States consider collecting data in order to:

- Assess the current threat of child sexual exploitation and abuse, how it is manifested and who is most at risk;
- Assess the country's vulnerability to this threat;
- Assess the current institutional response;
- Review and evaluate the implementation of applicable legislation and policies to assess compliance with international standards and good practice;
- Review the current ICT ecosystem response, including hotline reporting mechanisms and industry engagement; and
- Map the activity of other stakeholders engaged in this issue.⁸⁹

The collection of such data before drafting or amending legislation allows the drafters to be clear about the issues they are addressing, the aim of the legislation and priorities. To understand the true scale of online violence better, legislative drafters should also consider broader prevalence data, for instance data contained in population-based surveys which measure exposure to violence. Existing

large-scale surveys include, for example, the Global School-Based Student Health Survey, Demographic Health Surveys, Multiple Indicator Cluster Surveys and other dedicated surveys such as the Violence Against Children and Youth Surveys. Research which places the experiences of children and young people at its centre should be seen as particularly important in understanding the scale and nature of online child sexual abuse and exploitation, as law enforcement reporting data is likely to underestimate the prevalence of online child sexual abuse and exploitation.⁹⁰ It is helpful for the legislative drafters to understand the prevalence of online child sexual exploitation and abuse, the particular forms it takes within the country, the extent to which children are victims, the emerging trends and the legal gaps and barriers to the protection of children. This may require obtaining and analysing raw data from service providers in the digital environment, as well as data from law enforcement, investigation and prosecution authorities, the child protection system, service providers within civil society, and the judiciary at the national and subnational levels.



States should consider UNICEF's principles of responsible data handling when storing, analysing and making use of data related to children's experiences of online sexual abuse and exploitation. These principles include making sure that all data is participatory, that those controlling it are professionally accountable, data is people-centric, work is undertaken to prevent harms across the data life cycle and that data obtained is proportional, protects children's rights and is purpose-driven.⁹¹

Example: Republic of Korea

In 2017, 99.5 per cent of households in the country had access to the internet, with almost all children having access. The Republic of Korea is known to be a source, transit and destination country for the sexual exploitation and abuse of children, both online and in-person.⁹²

To understand the scale of this challenge better, the Ministry of Gender Equality and Family conducts a triennial nationwide survey to assess the prevalence of sexual abuse, including child sexual abuse. The Supreme Prosecutors' Office also compiles data on the number of recorded child sexual abuse offences.⁹³ Additionally, the Advocacy Centre for Online Sexual Abuse also gathers and publishes data on the number of victims of online sexual abuse and exploitation of adults and children.⁹⁴

✓ All justice stakeholders including law enforcement, investigation, prosecution and judicial bodies at the national and local levels should collect data on reported cases; cases dropped, diverted and prosecuted; convictions and measures imposed. In addition, data should be collected on the perpetrator and victim where possible, to allow policymakers to understand the demographic characteristics of the parties involved in online child sexual exploitation and abuse cases better. All data should be disaggregated by age, gender, disability, geographical location, ethnic and national origin, and socioeconomic background (as well as other protected characteristics, relevant to the local context).

✓ In many countries these data are difficult to obtain, and robust data collection systems are not in place. Where this is the case, in line with the OPSC Guidelines, new legislation should impose a duty on government and particularly on ministries to ensure that data is collected on all forms of child sexual exploitation and abuse including forms facilitated by technology.⁹⁵ This is likely to involve the Ministries leading State policy in the area of child protection and child justice, as well as Ministries leading on digitalization, culture, communication matters and national security.

✓ Personal data should be collected ethically, and in line with national and regional laws. All data collection, processing and storage should adhere to the highest possible standards for data protection for children, and in the absence of a higher national standard should follow the principles found in both the European General Data Protection Regulation and Chapter Two of the African Union Convention on Cyber Security and Personal Data Protection, namely: lawfulness, purpose limitation, data minimization, accuracy, secure storage, integrity and confidentiality, and accountability.

✓ Legislation should set out clear instructions for data processors and controllers to ensure data privacy and security. All prevalence data relating to children should be anonymized to ensure the confidentiality of children's personal information, and even anonymized data should be stored for the minimum time period required and with maximum security to minimize the risks of reidentification.

Ensure data on the trends and prevalence of online child sexual exploitation and abuse informs the development of primary and secondary legislation

The collection and sharing of data on the scale, issues and trends of online child sexual abuse and exploitation forms only a part of States parties' responsibilities to monitor children's rights. The remainder of the monitoring cycle involves analysing and using data to consult upon and inform the

development of State policy and legislation to address the issues identified.

Legislators should consider establishing clear mechanisms and processes to ensure decision-makers regularly receive available data. Collected data should be used on a systematic basis to inform the development of laws, policies and programmes to address gaps or inequities in the enjoyment of children's rights.

More information on the mechanisms which may be established for this purpose is set out below under the standard relating to **multi-sectoral bodies to share information and inform the development of laws and practices**.

Example: Ghana

In Ghana, in the run up to the adoption of the Cybersecurity Act 2020, UNICEF and its national partners worked together to advocate for legislative and policy reform to protect children from online child sexual exploitation and abuse. The 2017 *'Research Report on Risks and Opportunities Related to Online Child Practices: Ghana Country Report – December 2017'*,⁹⁶ carried out by the Ministry of Communications and UNICEF in partnership with

Global Kids Online, was used as an advocacy tool with stakeholders.⁹⁷

The research report and advocacy activities led to the development of a position paper by UNICEF and Ghana's Ministry of Gender, Children and Social Protection in 2018 covering legislative and policy gaps concerning children's safety online.⁹⁸ UNICEF and the Ministry used the paper to launch consultations with a broad range of stakeholders at the national level such as stakeholders within the telecommunications sector and within communities, including leaders of administrative divisions and teachers in schools. These engagements, which were rooted in evidence, raised awareness of gaps in the legislative framework and contributed to building the demand from stakeholders to amend the legislative and policy framework to protect children from online sexual exploitation and abuse. Findings of the study also informed the development of the National Child Online Protection Framework, which aims to bring relevant stakeholders across sectors together to address online child sexual exploitation and abuse.

Ensure children and young people's views are considered as a key element of the development of legislation related to online child sexual exploitation and abuse

International standards



Article 12 of the CRC

'States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.'

The CRC Committee recommends that States parties should respect, protect and fulfil the right of the child to be heard both in the content and process of legislative reform.⁹⁹ This includes identifying and addressing the emerging risks

that children face in diverse contexts, including by listening to their views on the nature of the particular risks they face.¹⁰⁰ Similar guidance is provided in the OPSC Guidelines, which calls upon States parties to *'make efforts to include child participation in the drafting process and in the implementation of legislative and policy measures, ensuring that the views of children are considered without discrimination, and that adults consulting with them have the necessary training and resources to carry out the consultations in an age-appropriate and gender-sensitive manner'*.¹⁰¹

The voices and opinions of children must be at the forefront of policy decisions taken on their behalf.



In line with the child's right to be heard under Article 12 of the CRC, decision-makers must ensure that child participation is integrated into the process of developing and monitoring legislation on online child sexual exploitation and abuse. This is essential, not only for respecting children as rights holders, but also for developing legislation that is effective in responding to the challenges faced by children and shaped by their lived experiences.

The CRC Committee General Comment No. 12 (2009) details key standards on the involvement of children in decision-making:

- *'The views expressed by children may add relevant perspectives and experience and should be considered in decision-making, policymaking and preparation of laws and/or measures as well as their evaluation.'*¹⁰²
- Participation should *'not only be a momentary act'* but a *'starting point for an intense exchange between children and adults on the development of policies, programmes and measures in all relevant contexts of children's lives'*.¹⁰³
- Children's views must be given effect, and, at a minimum, children should be informed of the outcome of their involvement in the development of legislation, understanding that *'feedback is a guarantee that the views of the child are not only heard as a formality, but are taken seriously'*.¹⁰⁴
- In the context of ensuring children are protected from all forms of violence, the CRC Committee encourages States parties to *'consult with children in the development and implementation of legislative, policy, educational and other measures to address all forms of violence'*. This includes ensuring the voices of children who are marginalized or disadvantaged are heard.¹⁰⁵

Where representative youth-led bodies for children exist, such as elected Youth Parliaments, Youth Councils and Children's Cabinets, efforts should be made to engage them directly in the development of legislation. CRC General Comment No. 12 elaborates that *'children should be supported and encouraged to form their own child-led organizations and initiatives, which will create space*

for meaningful participation and representation' on a wide range of issues, including online child sexual abuse and exploitation.¹⁰⁶ These structures should however be seen as *'one of many approaches'* to involving children in decision making.¹⁰⁷

Regional standards

The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Abuse (the Lanzarote Convention) also highlights the importance of child participation in the development of legislation. In line with Article 12 of the CRC, the Lanzarote Convention provides that: *'Each Party shall encourage the participation of children, according to their evolving capacity, in the development and the implementation of state policies, programmes or other initiatives concerning the fight against sexual exploitation and sexual abuse of children'*.¹⁰⁸

When considering how to best involve children and young people in the development of legislation, consideration should be given to:

- Age- and context- appropriate involvement of children to ensure that the issues discussed are in line with a child's maturity and understanding of the digital environment and issues related to abuse and exploitation;
- Ensuring the process of children's participation abides by the *'do no harm principle'* and makes a child's best interests the primary consideration. This is particularly important for children who may be victims of online abuse and exploitation;
- How to best inform children about potential legislation, including empowering and educating them on issues to allow them to make informed decisions influenced by their lived experiences;
- Ensuring children give their full and informed consent to being involved in any participation work;
- Use of child-friendly language (particularly in consultations or other formal processes) which is appropriate to the age and maturity of the children involved;

- How to ensure continuous involvement of children throughout the process, including closing feedback loops;
- Eliminating practical, political and social barriers to children’s engagement;
- Steps to engage actively with children from groups which have been marginalized or disadvantaged; and
- Raising the awareness of legislative drafters, civil servants, policymakers and other key stakeholders of the importance of including children and young people’s views.¹⁰⁹

Example: Republic of Ireland

The Lundy model for child participation is considered to be good practice when establishing models of children’s involvement in decision-making and forms the framework for the Government of Ireland’s Department of Children, Equality, Disability, Inclusion and Youth’s *‘National Framework for Children and Young People’s Participation in Decision Making’*. The framework aims to embed a culture of *‘participation with a purpose’* into decision-making by government and

third-sector bodies in the country, noting that: *‘It is important not to get stuck in the process of ‘doing’ participation, but to ensure that the purpose of involving children and young people in decision-making is to give them a voice on day-to-day activities and practices, or on the development of projects, programmes, services or policies.’*¹¹⁰

The framework contains a clear planning checklist, evaluation checklist, everyday spaces checklist and children and young people’s feedback forms, which together allow officials and those that work with children to practically include them in the development of legislation, policy and practice.¹¹¹

The Lundy model suggests four key elements that should be considered in any youth participation process: space, voice, audience and influence.¹¹² Figure 1 details the key considerations for implementing this in practice, taken from the everyday spaces checklist contained within the Irish Government’s child and young person’s participation strategy.

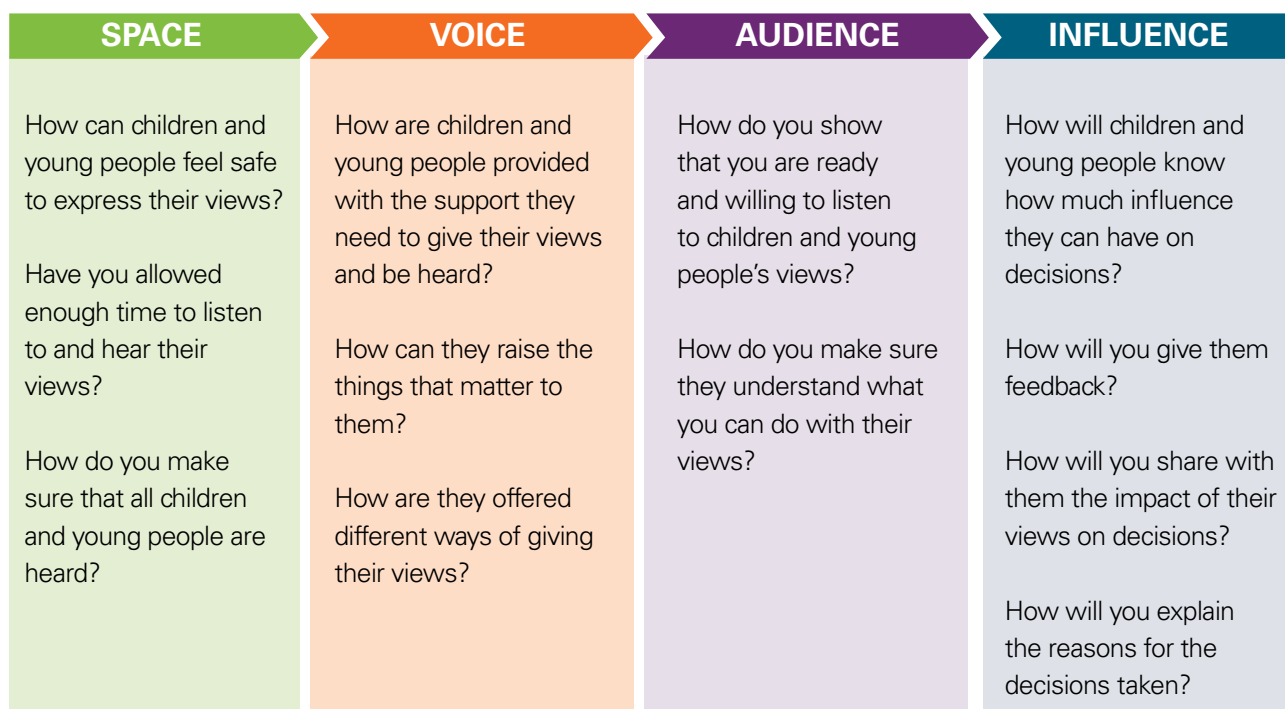


Figure 1: Lundy Model of Child Participation¹¹³

✓ The State should consider how a wide cross-section of children and young people could participate in the development of laws in a meaningful manner, including children and young people who may face exclusion from involvement, such as children with disabilities, children on the move, children from marginalized groups and others.

✓ General Comment No. 5 (2003) of the UN Committee on the Rights of the Child affirms that children with direct experiences of certain issues should be consulted as part of any participation process as *'the emphasis on "matters that affect*

them" in Article 12 (1) implies the ascertainment of the views of particular groups of children on particular issues - for example children who have experience of the juvenile justice system on proposals for law reform in that area'.¹¹⁴ Similarly, States should consider how children who have experienced online sexual abuse and exploitation can have their voices heard throughout the process of developing legislation and are provided with appropriate support to do so. It is also important to consult and seek input from adults who were sexually exploited or abused online as children, as their lived experience can often provide valuable insight.

Civil society expertise, including from NGOs, industry and academia, **should** be involved in the development of legislation related to online child sexual exploitation and abuse

CRC General Comment No. 25 (2021) provides that States should *'systematically involve civil society, including child-led groups and non-governmental organizations working in the field of children's rights and those concerned with the digital environment, in the development, implementation, monitoring and evaluation of laws, policies, plans and programmes relating to children's rights'*.¹¹⁵

The OPSC Guidelines also recommend that States undertake *'online-specific analyses, research and monitoring to improve their understanding of online sale, sexual exploitation and sexual abuse of children and to develop responses to online offences in close collaboration with the relevant industries and organizations'*.¹¹⁶

Expert research and data that is collected and analysed by civil society, national human rights bodies, industry and academia are critical tools, allowing decision-makers to understand issues and trends related to online child sexual abuse and exploitation. At the international, regional, national and subnational levels, national human rights institutions (NHRIs), NGOs, academics and industry experts produce high quality research across a variety of topics related to children's safety in the digital environment.

Government departments should share information between themselves and also encourage NGOs running national helplines to share data on online child exploitation and abuse with departments responsible for communications technology and child protection. During the Covid-19 pandemic, for example, data from national helplines was able to show government that there was a marked increase in online child sexual abuse and exploitation of children.¹¹⁷ In many countries, strong relationships and frequent communication between NGOs and governments have resulted in a more coordinated response effort to tackle this issue.

✓ Where limited information is known on a particular topic, governments should consider commissioning qualitative and quantitative research in partnership with NGOs, business and academia in order to better understand the experiences of children and the latest trends and challenges in responding to online child sexual exploitation and abuse.

Multi-sector monitoring bodies **should** share information and inform the development of policy and practice

As part of *'general measures of implementation'* under Article 4 of the CRC, the CRC Committee recommends that State parties establish *'coordinating and monitoring bodies – governmental and independent'*.¹¹⁸ The purpose of the governmental bodies is to ensure, broadly, *'effective implementation'* of the CRC and the enjoyment of its rights for all children within the State party's jurisdiction,¹¹⁹ which includes the right to protection from online child sexual exploitation and abuse. Although the CRC Committee does not prescribe structures or arrangements for such bodies, it states that, a *'special unit, if given high-level authority reporting directly, for example, to the Prime Minister, the President or a Cabinet Committee on children can contribute both to the overall purpose of making children more visible in Government and to coordination to ensure respect for children's rights across Government and at all levels of Government'*.¹²⁰ Such a unit can be given responsibility, not only for developing and coordinating the implementation of strategies relating to children but also *'monitoring [their]... implementation'*.¹²¹ In order to function effectively this body should be provided with a secretariat, a defined budget, strategy, terms of reference and clear reporting cycle.¹²² Mechanisms may also be introduced to integrate the voices of civil society, academia and children to strengthen accountability, inter-sectoral coordination and expertise.¹²³

Multi-sector monitoring bodies may also be established at the national level to share information and inform the development of policy and practice concerning the protection of children in the digital environment. Civil society, academia and other experts should be included as members of such bodies. This will enable a greater *'real time'* understanding of the scale and nature of online child sexual abuse and exploitation. The WeProtect Model National Response suggests that to ensure *'good governance'*, a Government-led cross-sector national body or bodies should be developed which *'brings together those with a responsibility for tackling online child sexual abuse and exploitation'*.¹²⁴ The remit of such governance mechanisms can vary,

reflecting political contexts and institutional set ups; some focus on child sexual exploitation and abuse online, while others tackle the issue as part of a broader remit such as violence against children, child protection or digital safety and security.¹²⁵ Such a body aids in the sharing of expertise and knowledge related to combatting online sexual abuse and exploitation and coordinated work on relevant national programmes.¹²⁶

Example: United Kingdom of Great Britain and Northern Ireland

In the United Kingdom the UK Council on Internet Safety is a body led by the UK Government's Department for Digital, Culture, Media and Sport, the Department for Education and the Home Office as a collaborative effort between government, the tech industry and civil society to tackle harm caused in the digital environment, including online harms experienced by children, such as cyberbullying and sexual exploitation.¹²⁷

The Council has an Evidence Group which was founded in 2011 and is comprised of 15 experts from across academia, government, NGOs and industry.¹²⁸ Believing that *'research findings are vital to provide the evidence base to inform stakeholder actions designed to improve children's online safety'*, the group collates information in order to give a timely, critical and rigorous account of the relevant research by providing two-page *'highlight'* reports of relevant studies to the Council.¹²⁹

The Council's positioning as an independent body led by the government puts it in a unique position to act as a *'research watchdog'* and inform policy and practice on children's online safety in the UK. Most recently this has included providing evidence to inform the development of the new UK Online Safety Bill (2022). The role of the Evidence Group was to *'make sure that the policy was evidence-based'*.¹³⁰

More detail on the involvement of civil society in the development of legislation can be found in **Part 4: Stakeholder engagement and catalysts for legal reform**. Details on the role of independent monitoring bodies can be found in **Part 10: Independent monitoring and regulation**.

✓ States should consider developing formal relationships, in the form of multi-sector monitoring bodies or equivalent bodies, between government, NGOs, academia and industry both for the sharing

of information and the development of policy and practice.

✓ Children should be invited to contribute to the multi-sector coordination body. Efforts should be made to ensure children are involved in a meaningful way, including ensuring they are supported in the process and decision makers take the views of children seriously and act on them where appropriate.

Existing legislation **should** be monitored and evaluated to ensure it complies with international and regional standards and best practice

General Comment No. 25 emphasizes the need for continuous evaluation and monitoring of existing legislation, known as post-legislative scrutiny. In addition, the CRC Committee calls for the establishment, coordination and regular monitoring and evaluation of frameworks for the referral of violations and the provision of effective support to children who are victims.¹³¹

Post-legislative scrutiny can best be described as the stage at which the legislature asks itself the question: are the laws of a country producing the expected outcomes, to what extent, and if not, why not?¹³² Its purpose is to *'review both the enactment of a law and its impact on society'*¹³³ and to ensure that legislation meets its intended aims and is of a high quality. In practice there are two key components of post-legislative scrutiny:

1. Evaluation – to assess technically whether a piece or multiple pieces of legislation, when taken together, have been implemented effectively and have achieved their intended aims; and
2. Monitoring – to examine the application of a piece of legislation and resulting secondary legislation (i.e. Standard Operating Procedures, Manuals and Guidelines, etc.) against its intended policy outcomes.

In the context of prevention and response to the continually evolving issue of online child sexual exploitation and abuse, the importance of both evaluation and monitoring cannot be understated. This may include continually reviewing laws to assess their effectiveness in practice, ensuring they are up-to-date with the latest data and research, remain informed by the lived experiences of their beneficiaries, keep pace with new ICTs and do not have any unintended consequences.

✓ States should consider integrating systematic post-legislative scrutiny into their national monitoring mechanisms. It is recommended that the process of post-legislative scrutiny takes place no later than three years after the enactment of a piece of legislation.¹³⁴ In different national contexts, different forums may be responsible for this oversight function, including committees, commissions, external working bodies or independent state agencies. The body tasked with the research should be independent in its mandate, be inclusive of all political parties and have the power to make recommendations to legislators, where necessary, to allow for legal amendments or other changes to be brought forward by Parliament.

Example: **Mongolia**



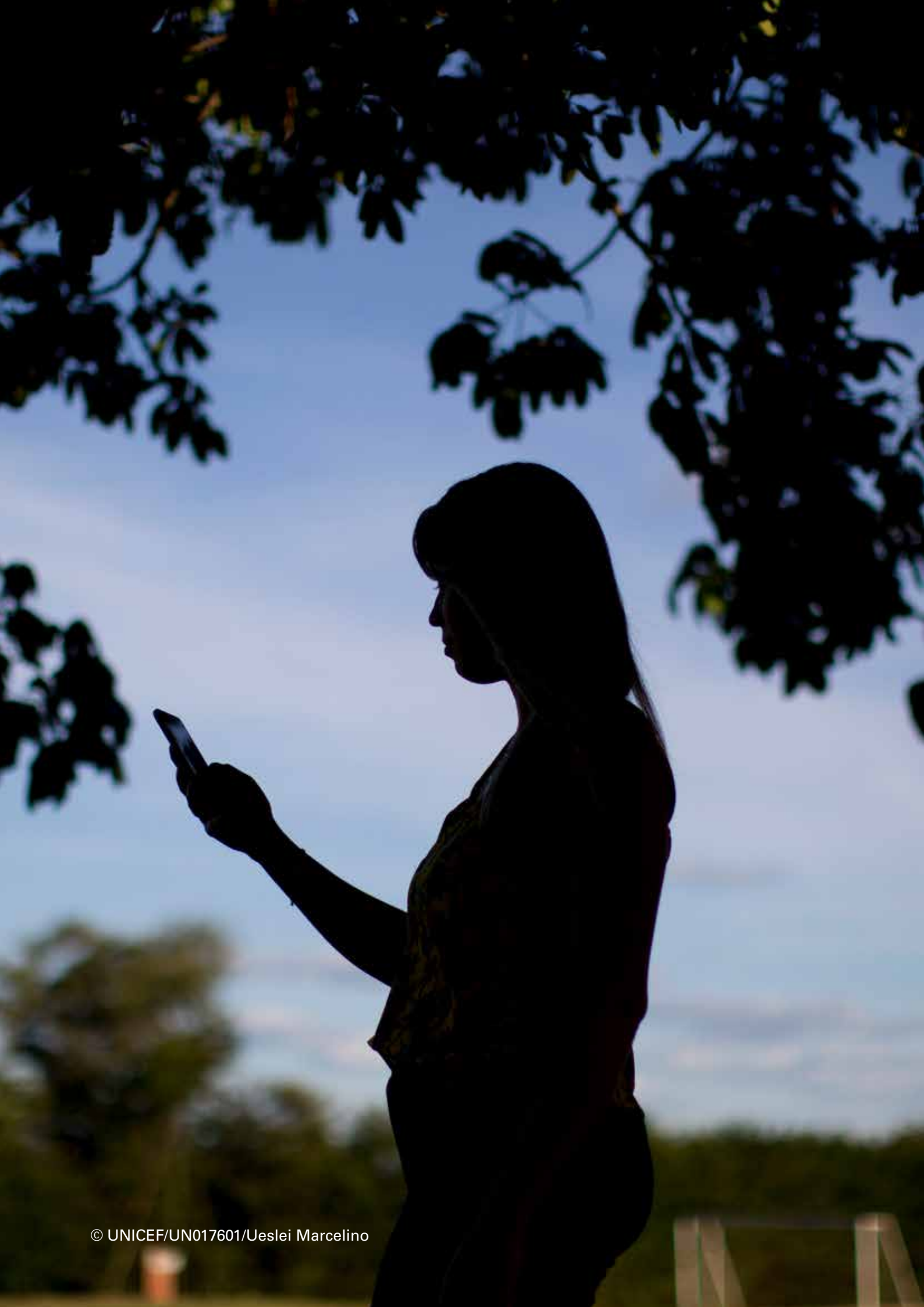
Under Article 51 of the Mongolian Law on Legislation all newly enacted pieces of legislation must be evaluated to assess their implementation and unintended consequences.¹³⁵ In 2020-21 with the support of UNICEF, the Government of Mongolia commissioned an evaluation of the 2016 Law on Child Protection. The Law on Child Protection, together with the Law on the Rights of the Child and the Domestic Violence Law, were enacted in order to provide comprehensive protection to all children in Mongolia.¹³⁶ The law set out, for the first time, the roles and responsibilities of duty bearers across sectors in preventing and responding to violations of the rights of the child.

The evaluation was designed to highlight lessons learned, identify areas for improvement, record the achievements of key stakeholders and duty bearers, and make recommendations to improve the efficiency and effectiveness of the implementation of the Law on Child Protection, including how the child protection system prevented and responded to online child sexual exploitation and abuse.¹³⁷

Following the evaluations publication in January 2021, on 8 March 2021 a coalition of parliamentarians in Mongolia submitted draft legislation in line with these recommendations to amend the Law on Child Protection to the State Great Khural (the national parliament).¹³⁸

Endnotes

- 84 CRC General Comment No. 25 (2021), para. 23.
- 85 Ibid., para. 30.
- 86 ACRWC General Comment No. 7 (2021), para. 132.
- 87 The CRC Committee's Guidelines regarding the implementation of OPSC are not internationally binding but should be regarded as highly influential as they interpret the OPSC, which has been acceded to or ratified by all but eight States.
- 88 UNCRC Committee 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, 10 December 2019, para. 20(b)-(c).
- 89 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, November 2016, <www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf>, accessed 5 January 2022.
- 90 An example is the Disrupting Harm project, funded by the End Violence Fund and implemented by ECPAT, INTERPOL and UNICEF, which has generated evidence in 13 countries so far on children's experiences of online child sexual exploitation and abuse, and how national protection systems are responding, <https://www.end-violence.org/disrupting-harm>, accessed 5 May 2022.
- 91 UNICEF, Responsible Data for Children, <www.rd4c.org/principles>, accessed 5 January 2022.
- 92 US State Department, 2021 Trafficking in Persons Report: South Korea, <www.state.gov/reports/2021-trafficking-in-persons-report/south-korea>, accessed 30 March 2022.
- 93 The Economist Intelligence Unit, Out of the shadows: Shining light on the response to child sexual abuse and exploitation, South Korea Country Profile, 2020, <www.outoftheshadows.eiu.com>, accessed 30 March 2022.
- 94 Online individual interview, Korea Legislation Research Institute, 31 March 2022.
- 95 OPSC Guidelines, para. 20.
- 96 Ghana Country Report, December 2017, <www.unicef.org/ghana/media/1791/file/Risks%20and%20Opportunities%20-%20Child%20Online%20Protection.pdf>
- 97 Online individual interview, UNICEF Ghana, 29 September 2021.
- 98 UNICEF, Risks and Opportunities related to child online practices: Ghana Country Report, December 2017, <www.unicef.org/ghana/media/1791/file/Risks%20and%20Opportunities%20-%20Child%20Online%20Protection.pdf>, accessed 28 May 2022.
- 99 CRC General Comment No. 25 (2021), paras. 14 and 17.
- 100 Ibid., para. 14.
- 101 OPSC Guidelines, para. 12.
- 102 CRC General Comment No. 12 (2009), para. 12-13.
- 103 Ibid.
- 104 Ibid., para. 45.
- 105 Ibid., para. 118.
- 106 Ibid., para. 128.
- 107 Ibid., para. 127.
- 108 Lanzarote Convention, Article 9 (1).
- 109 For more on participation, see Council of Europe, Handbook for policy makers on the rights of the child in the digital environment, 2019, <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>, accessed 12 May 2022 and Council of Europe Child Participation Assessment Tool (CPAT), Appendix, p. 28, <https://rm.coe.int/16806482d9>.
- 110 Government of Ireland, Department of Children and Youth Affairs, National Strategy on Children and Young People's Participation in Decision-Making 2015-2020, 13 March 2019, p. 6, <www.gov.ie/en/publication/9128db-national-strategy-on-children-and-young-peoples-participation-in-dec/>, accessed 1 April 2022.
- 111 Hub na nÓg., Participation Framework, 2019, <www.hubnanog.ie/participation-framework/>, accessed 1 April 2022.
- 112 Lundy, Laura, 'Voice' Is Not Enough: Conceptualising Article 12 of the United Nations Convention on the Rights of the Child', British Educational Research Journal, vol. 33, no. 6, 2007, pp. 927-42.
- 113 Ibid.
- 114 CRC General Comment No. 5 (2003), para. 12.
- 115 CRC General Comment No. 25 (2021), para. 34.
- 116 OPSC Guidelines, para. 38.
- 117 INTERPOL, Threats and Trends Child Sexual Exploitation and Abuse: Covid-19 Impact, September 2020, p. 9, <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse>, accessed 14 May, 2022.
- 118 Committee on the Rights of the Child, General Comment No. 5 (2003): General Measures of Implementation of the Convention on the Rights of the Child, CRC/GC/2003/5 (2003), para. 9.
- 119 Ibid., para. 37.
- 120 Ibid., para. 39.
- 121 Ibid., para. 39.
- 122 See, for example, Hamilton, C. et al., Programme-Informing Evaluation of the Child Rights Monitoring System in Montenegro and Planned Approach to Child Rights Monitoring under the 2017-2021 Country Programme, UNICEF Country Office in Montenegro, Podgorica, 28 March 2018, p. 20.
- 123 Ibid.
- 124 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response, 2016, p. 3, [https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf](http://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf)
- 125 WeProtect Global Alliance, Framing the future: How the Model National Response framework is supporting national efforts to end online child sexual exploitation and abuse, 2022.
- 126 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response, 2016, p. 3, [https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf](http://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf)
- 127 UK Council for Internet Safety, About Us, UK Government, <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>, accessed 14 May 2022.
- 128 UK Safer Internet Centre, Evidence Group Members, <https://saferinternet.org.uk/evidence-group-members> < accessed 14 May 2022.
- 129 UK Safer Internet Centre, Research Highlight Series, <<https://saferinternet.org.uk/research-highlight-series>>, accessed 7 March 2022.
- 130 Online individual interview, UK Council for Internet Safety, 22 March 2022.
- 131 CRC General Comment No. 25 (2021), paras. 44 – 46.
- 132 De Vrieze, Franklin, A Guide to Post-Legislative Scrutiny, Westminster Foundation for Democracy, 23 July 2018, p. 9, <www.wfd.org/what-we-do/resources/guide-post-legislative-scrutiny>, accessed 7 March 2022.
- 133 De Vrieze, Franklin, Principles of Post-Legislative Scrutiny by Parliaments, January 2018, p. 6, <www.agora-parl.org/resources/library/principles-post-legislative-scrutiny>, accessed 7 March 2022.
- 134 Ibid.
- 135 Law on Legislation (2017), Article 51.
- 136 Aplan, Kara et al., Evaluation of the Implementation of the Law on Child Protection (LCP) in Mongolia, UNICEF Mongolia, January 2021, p. 4, <www.researchgate.net/publication/350021218_Evaluation_of_the_Implementation_of_the_Law_on_Child_Protection_LCP_in_Mongolia>, accessed 7 March 2022.
- 137 Ibid., p. 28.
- 138 Unurzul, M., Bills to amend the Law on Child Protection and the Law on Gender Equality submitted, Montsame, 9 March 2021, <www.montsame.mn/en/read/256007>, accessed 15 March 2022.



4. Stakeholder engagement and catalysts for legal reform

Checklist of minimum and recommended standards

Advocacy and other communications strategies **should** raise awareness of child sexual exploitation and abuse including forms facilitated by the use of information and communication technologies, based on up-to-date research and information

Links to broader and/or related initiatives concerning the protection of children, such as movements to address violence against women and/or children, or broader cybersecurity or digitalisation initiatives, **should** be identified and used as entry points for stakeholder engagement and legislative reform

Collaboration with key strategic stakeholders within government **should** be strengthened in order for government to take the lead in the development of policy and legislative reforms

Consider leveraging the influence and leadership of regional and international inter-governmental organizations to promote national legal reforms

Stakeholder engagement is a key part of any strategy for legal reform. Part 4 of this Global Guide highlights key considerations for stakeholder engagement, when planning and implementing legislative reform efforts to protect children from online child sexual exploitation and abuse.

4.1 Detail of minimum and recommended standards

Advocacy and other communications strategies **should** raise awareness of child sexual exploitation and abuse including forms facilitated by the use of information and communication technologies, based on up-to-date research and information

Advocacy may be described as an *'organized effort to inform and motivate leadership to create an enabling environment for achieving programme objectives and development goals'*.¹³⁹ It is important for promoting the development of new laws or changes to existing laws as well as helping to *'redefine public perceptions'* and influence funding decisions.¹⁴⁰ Advocacy activities can stimulate changes in attitudes and behaviours at all levels

of society but generally focus on stakeholders at the policy and *'systems'* level such as government ministries, parliamentarians, national civil society organizations and business groups, among others.

Advocacy strategies may also form part of a wider communications strategy, targeting individual members of the public, including children, parents, carers and teachers, and community-level

stakeholders and institutions. Communication strategies play an important part in creating a ‘demand’ within society for children’s rights to be respected, protected and fulfilled in the digital environment, which in turn encourages policy and systems level stakeholders to develop legislation in this area. For more details on other types of communication strategies, such as training for professionals and practitioners and education programmes for children, parents and carers on preventing and responding to online child sexual exploitation and abuse, please see **Part 11: Implementation of legislation.**

High-profile child abuse cases or tragedies may act as catalysts for legal reform by prompting policymakers and leaders to take action in response to public outrage.

Example: United Arab Emirates

The tragic case of Wadeema, an eight (8) year old Emirati girl who was tortured and murdered by her father and his girlfriend, and the torture of her younger sister, Mira, sparked outrage in the United Arab Emirates and led to the development of national child rights legislation. Federal Law No. 3 of 2016 on Child Rights, also known as ‘Wadeema’s Law’, affirms the child’s right to protection and provides a skeleton framework for providing child protection interventions by the State.¹⁴¹

Although reports of Wadeema’s suffering did not highlight any instances of online sexual exploitation and abuse, Wadeema’s Law recognizes a child’s ‘*exposure to exploitation or sexual abuse*’ as grounds for child protection interventions.¹⁴² It also contains a provision specifically prohibiting certain acts relating to ‘*child pornography*’, including possession, regardless of whether there is an intent to

distribute. The definition of ‘*child pornography*’ specifically contemplates online means, as follows: ‘*the production, display, publication, possession or circulation of a picture, film or drawing through any means of communication, social media platforms or other means where the child is shown in a disgraceful manner in a sexual act or sexual show, whether such act is real, virtual or simulated*’.¹⁴³ (Please refer to **Part 6 on minimum standards concerning the criminalization of child sexual abuse material.**)

Example: Republic of Korea

Public outcry over the ‘*nth room*’ and ‘*Welcome To Video*’ cases in the Republic of Korea led to legislative amendments to strengthen the protection of children from online sexual exploitation and abuse.

The ‘*nth room*’ refers to the investigation and prosecution of an organized criminal gang that exploited 74 people including 16 girls into sharing sexual videos which were then posted in pay-to-view chatrooms used by at least 10,000 people.¹⁴⁴ ‘*Welcome to Video*’ was a website on the dark web on which people traded child sexual abuse materials involving children as young as six months old using bitcoin currency. The victims included children in the USA, Spain and the UK, though the alleged administrator of the site was in the Republic of Korea.¹⁴⁵

The legislative reforms included two new provisions in the Act on the Protection of Children and Youth against Sex Offences on 23 March 2021 concerning a new crime of online grooming of children and adolescents (Article 15-2) and increased powers for law enforcement to undertake covert operations to investigate digital offences against children and young people (Article 25-2).



Public outcries may provoke calls for measures which do not necessarily comply with international human rights standards. Particular care should therefore be taken to avoid ‘*knee-jerk*’ reactions that are not supported by evidence, or which erode the State’s compliance with its international human rights obligations.

Links to broader and/or related initiatives concerning the protection of children, such as movements to address violence against women and/or children, or broader cybersecurity or digitalization initiatives, **should** be identified and used as entry points for stakeholder engagement and legislative reform

Initiatives related to combating sexual exploitation and abuse of children or violence more generally should be used, where appropriate, as entry points for dialogue and stakeholder engagement. Initiatives relating to cybersecurity and digital transformation may also present opportunities.

One example of a global initiative is the WeProtect Global Alliance: a group of 98 government members (as well as 54 company members, 67 civil society organizations and 9 international organizations).¹⁴⁶ All governmental members have signed up to the Alliance's commitments and to progressing their implementation, including the Alliance's Model National Response on Preventing and Tackling Child Sexual Exploitation and Abuse. The Model National Response sets out a series of 21 '*capabilities*' that are needed to protect children from sexual exploitation and abuse including forms facilitated by ICTs.¹⁴⁷ Capability 3 is particularly relevant to this Global Guide: the development of '*[c]omprehensive and effective domestic legislation to protect children from all forms of sexual exploitation and abuse – both online and offline*'.¹⁴⁸

The Global Partnership to End Violence against Children's '*Pathfinding*' initiative is a further example of a potential entry point. Under this initiative, leaders of '*pathfinding countries*' make a formal, public commitment to take action to end all forms of violence against children.¹⁴⁹ Once the End Violence Secretariat has approved a country's pathfinding status, the government of the pathfinder country is expected to develop an evidence-based and costed national action plan within 18 months, setting out the country's commitments to address violence against children over a period of three to five years. One of the key components for the action plan relates specifically to ensuring that legislation criminalizes all forms of sexual abuse and exploitation of children.¹⁵⁰

Other potential entry points include national strategies and programmes to address violence against women and girls, such as the Spotlight Initiative.¹⁵¹

Example: Zimbabwe

In 2021, Zimbabwe adopted the Data Protection Act No. 5 of 2021, which criminalizes specific means of online child sexual exploitation and abuse and introduces procedural provisions to facilitate the investigation of such crimes. As a member of the WeProtect Global Alliance, the government (led by the Ministry of Information Communication Technology, Postal and Courier Services) and UNICEF identified a need to protect children from these risks online and established a national, multi-sectoral committee – the Committee for Child Online Protection – to develop a strategy for implementing the WeProtect Global Alliance's Model National Response.¹⁵² The establishment of this Committee provided a vehicle for cross-sectoral engagement, using the membership of the WeProtect Global Alliance and the Model National Response as an entry point to strengthen the legislative framework. UNICEF further joined forces with UN Women and the United Nations Population Fund to advocate for the protection of both women and children from gendered online violence through legal reform, using the Spotlight Initiative as a vehicle for joint action. This resulted in dedicated provisions against gendered online violence.

Example: Association of Southeast Asian Nations

The ASEAN States have recently developed a regional framework to strengthen national efforts to protect children from online child sexual exploitation and abuse, including through legislative reform (see below for details).

This framework includes a Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN¹⁵³ and Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN.¹⁵⁴ To develop these standards, several related initiatives were used as entry points for advocacy and stakeholder engagement.

These included ASEAN's broader framework for combating violence against children, most notably the Declaration on the Elimination of Violence against Women and the Elimination of Violence against Children in ASEAN 2013¹⁵⁵ and ASEAN Regional Plan of Action on the Elimination of Violence against Children 2015.¹⁵⁶ The Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN also draws on standards from other regions, including the Budapest Convention and Lanzarote Convention from the Council of Europe, and models of good practice, including the WeProtect Global Alliance's Model National Response.

Collaboration with key strategic stakeholders within government **should** be strengthened in order for government to take the lead in the development of policy and legislative reforms

Though it is important to promote inclusion and build consensus among stakeholders when advocating for legislative reform, it is also important to develop strategic partnerships within government to support advocacy efforts and to *'take the lead'* with the drafting of the new law or legal amendments.

The protection of children from online child sexual exploitation and abuse requires a robust technical understanding of the digital environment and it is important to build strategic links with stakeholders in the digital sector to secure their participation in the consultation process. Such expertise and strategic positioning often rest within government ministries or departments responsible for digital, culture, communications, or other similar mandate. However, the legislative reform efforts also require in-depth knowledge of children's rights and engagement with stakeholders active on this issue, which often (though not necessarily) rest with the government ministry or department responsible for children's rights or child protection issues (for example, the Ministry of Social Welfare, Ministry of Education or equivalent ministry, institution or department).

✓ The identification of a ministry within government to take the lead in promoting a new law or legislative amendments requires careful consideration and should be considered together the form in which the legislative reforms will be enacted (see further **Part 5: Methods of legislative reform**).

✓ The appointment of a lead ministry does not negate the need to promote cross-sectoral collaboration with a range of stakeholders across the ICT, cybersecurity, child protection, business and justice sectors, the involvement of which is essential to provide a holistic response to protecting children from online sexual exploitation and abuse.

The case study below provides an example of how these considerations have played out in practice in the run-up to the adoption of legislative reforms.

Example: Ghana

The Ministry of Gender, Children and Social Protection in Ghana was leading the development of a new Children’s Bill, which was intended to contribute towards the implementation of Ghana’s Child and Family Welfare Policy 2015. The development of the Children’s Bill provided an entry point to introduce provisions relating to the protection of children from online child sexual exploitation and abuse and contribute towards bridging the gaps highlighted in the 2018 position paper¹⁵⁷ on legislative and policy gaps concerning children’s safety online.¹⁵⁸

At the same time, the Ministry of Communications was developing a Cybersecurity Bill (which was eventually adopted as the Cybersecurity Act in December 2020). The Cybersecurity Bill was scheduled to enter into law in 2020, before the Children’s Bill (which, at the time of writing, remains a Bill). The speedier passage of the Cybersecurity Bill through Parliament was one of the reasons why the provisions relating to crimes of online child sexual exploitation and abuse were moved from the Children’s Bill and incorporated into the Cybersecurity Bill.¹⁵⁹

The relocation of the provisions from the Children’s Bill to the Cybersecurity Bill also had advantages in terms of stakeholder engagement. It provided opportunities for policymakers and advocates to engage closely with sector-specific stakeholders, such as Ghana’s National Cybersecurity Advisor and, in particular, with ICT service providers in the private sector. The involvement of the service providers was seen as essential for combating online child sexual exploitation and abuse and it was likely they would be more willing to get involved in consultations on a Cybersecurity Bill than consultations on a Children’s Bill.¹⁶⁰ The Cybersecurity Bill also facilitated stakeholder coordination on related cybercrime reforms, such as combating online human trafficking, the provisions for which overlap with issues relating to the investigation and prosecution of online child sexual exploitation and abuse. Further, this approach facilitated

cross-sectoral efforts to develop the institutional framework and administrative capacities to handle individual cases of online child sexual exploitation and abuse in practice, including the establishment in 2020 of the Child Online Protection Portal at the Accra Digital Center by the Ministry of Communications and Digitalisation, through Ghana’s National Cybersecurity Center.¹⁶¹



Where there is a lack of support for legislative reform within government, consider introducing a private member’s bill (for jurisdictions which allow this).

Certain jurisdictions allow members of the legislature who are not members of the executive branch to table a draft law for consideration by the legislature. Even if the bill does not become law, this approach can provide an entry point to raise awareness of the need for legislative reform, generate publicity and contribute towards promoting buy-in with government.

Example: United Kingdom of Great Britain and Northern Ireland

On 19 November 2021, Baroness Kidron, a member of the second chamber of the UK Parliament - the House of Lords, proposed a private member's bill titled the Age Assurance (Minimum Standards) Bill.¹⁶² The Bill required Ofcom, the UK's communications regulator, to produce a code of conduct setting out mandatory minimum standards for age assurance systems online – namely, systems which purport to estimate or verify the age or age range of a

user in order to protect children from harmful content, including pornography and sexual abuse materials.¹⁶³ Although the Bill was rejected due to lack of government support, the debates served to raise awareness of the risks children face online and contribute to the debates on whether or not to introduce mandatory age assurance requirements on internet service providers under the Online Safety Bill. See **Part 7: Duties and responsibilities in relation to business** for more details on mandatory age assurance in the Online Safety Bill.

Consider leveraging the influence and leadership of regional and international inter-governmental organizations to promote national legal reforms

International and regional inter-governmental organizations can play a key role in advocating and setting standards for legislative and policy developments to protect children from online sexual exploitation and abuse.

Example: Association of Southeast Asian Nations

The ASEAN States (Brunei Darussalam; Cambodia; Indonesia; Lao PDR; Malaysia; Myanmar; Philippines; Singapore; Thailand; and Viet Nam) have been a key vehicle in advocating for legislative reforms at the national level. In 2019, the ASEAN States signed the Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN.¹⁶⁴ The Declaration expresses the commitment of ASEAN States to protect children from all forms of online exploitation and abuse. It prioritizes seven measures, the first of which is to *'promote, develop, and implement comprehensive national legal frameworks in each ASEAN Member State and work towards improving child protection standards and policies on all forms of online exploitation and abuse across ASEAN Member States'*.¹⁶⁵

The ASEAN States furthered their commitments in October 2021 by signing the Regional Plan

of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN.¹⁶⁶ The Regional Plan of Action includes seven focus areas, which are in turn broken down into a series of activities. Focus area one relates to legislative reform and includes meeting minimum legal standards listed in Annex 3 of the Regional Plan of Action.

The Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN has significant potential to progress national-level legislative reforms in the region in the coming years.

Endnotes

- 139 UNICEF, 2017 Report on Communication for Development (C4D) Global Progress and Country Level Highlights Across Programme Areas, <www.unicef.org/media/47781/file/UNICEF_2017_Report_on_Communication_for_Development_C4D.pdf>, p. 9.
- 140 Ibid.
- 141 Federal Law No. 3 of 2016 on Child Rights (Wadeema's Law), Article 2.2 and Chapter 8; Website of the United Arab Emirates, Children's safety, www.khda.gov.ae/CMS/WebParts/TextEditor/Documents/Children_Law_English.pdf, accessed 22 April 2022.
- 142 Federal Law No. 3 of 2016 on Child Rights (Wadeema's Law), Article 33.5.
- 143 Ibid., Article 1.
- 144 BBC News, Cho Ju-bin: South Korea chatroom sex abuse suspect named after outcry, 25 March 2020, <www.bbc.co.uk/news/world-asia-52030219>, accessed 4 April 2022.
- 145 Hollingsworth, Julia, How Bitcoin transactions were used to track down the 23-year-old South Korean operating a global child exploitation site from his bedroom, 20 October 2019, <www.edition.cnn.com/2019/10/19/asia/south-korea-child-exploitation-international-police-intl-hnk/index.html>, accessed 4 April 2022.
- 146 WeProtect Global Alliance, The Alliance, <www.weprotect.org/alliance/>, accessed 12 May 2022.
- 147 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, November 2016, p. 1.
- 148 Ibid, p. 7. Another related entry point is the WeProtect Global Alliance's Global Strategic Response framework to eliminate online child sexual exploitation and abuse. The framework calls for governments to demonstrate political will, develop legislation and work collaboratively with international partners to eliminate online child sexual exploitation and abuse.
- 149 End Violence against Children, Pathfinding Countries, <www.end-violence.org/pathfinding-countries>, accessed 9 November 2021.
- 150 INSPIRE, Seven Strategies for Ending Violence against Children, Luxembourg 2016, <https://www.who.int/publications/i/item/inspire-seven-strategies-for-ending-violence-against-children>, accessed 18 February 2022.
- 151 A global, multi-year partnership between the European Union and the United Nations to eliminate all forms of violence against women and girls by 2030; Spotlight Initiative, What we do, <www.spotlightinitiative.org/what-we-do>, accessed 18 February 2022.
- 152 Online individual interview, UNICEF Zimbabwe, 23 September 2021.
- 153 Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, 2019, <www.asean.org/wp-content/uploads/2019/11/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf>, accessed 16 March 2022.
- 154 Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN, https://asean.org/wp-content/uploads/2021/11/4.-ASEAN-RPA-on-COEA_Final.pdf, accessed 12 May 2022.
- 155 Declaration on the Elimination of Violence against Women and the Elimination of Violence against Children in ASEAN, 2013, <www.ohchr.org/sites/default/files/Documents/Issues/Women/WG/ASEAN-declarationVaW_violenceagainstchildren.pdf>, accessed 16 March 2022.
- 156 ASEAN Regional Plan of Action on the Elimination of Violence against Children, 2015, https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/document_files/asean_regional_plan_of_action_on_elimination_of_violence_against_children_adopted.pdf, accessed 24 May 2022.
- 157 Children's Online Safety Concerns in Ghana, www.unicef.org/ghana/media/1806/file/Child%20Online%20Safety%20-%20Legislation%20and%20Policy%20Gaps.pdf
- 158 Online individual interview, UNICEF Ghana, 29 September 2021.
- 159 Ibid.
- 160 Ibid.
- 161 Ibid. For more on the Online Portal, please refer to the Ministry of Communications and Digitalisation website, <www.moc.gov.gh/child-online-protection-portal-launched>, accessed 5 April 2022.
- 162 Hansard, Age Assurance (Minimum Standards) Bill [HL], Volume 816: debated on Friday 19 November 2021, <[https://hansard.parliament.uk/lords/2021-11-19/debates/B5044809-8B71-4C4A-82F8-5BA496610C54/AgeAssurance\(MinimumStandards\)Bill\(HL\)](https://hansard.parliament.uk/lords/2021-11-19/debates/B5044809-8B71-4C4A-82F8-5BA496610C54/AgeAssurance(MinimumStandards)Bill(HL))>, accessed 28 March 2022.
- 163 Ibid.
- 164 Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, 2019, <www.asean.org/wp-content/uploads/2019/11/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf>, accessed 16 March 2022.
- 165 Ibid., para. A, <www.asean.org/wp-content/uploads/2019/11/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf>, accessed 16 March 2022.
- 166 Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN, https://asean.org/wp-content/uploads/2021/11/4.-ASEAN-RPA-on-COEA_Final.pdf, accessed 12 May 2022.



5. Methods of legislative reform

Checklist of minimum and recommended standards

The method of legislative reform (amending an existing law, developing a new law or a combination of both) and the thematic framework (criminal code, cybercrime, child protection, online safety, and/or other) in which to introduce the reforms **should** be identified

Consequential amendments to other laws **should** be identified

5.1 Detail of minimum and recommended standards

The method of legislative reform (amending an existing law, developing a new law or a combination of both) and the thematic framework (criminal code, cybercrime, child protection, online safety, and/or other) in which to introduce the reforms **should** be identified

When embarking on the legislative reform process, there are a number of possibilities: amending an existing law, developing a new law or a combination of the two. It may also be that the necessary provisions already exist in law, but are spread across a number of different instruments, and what is needed is the consolidation of these provisions into one coherent law.

Stakeholders will also need to consider the thematic *'framework'* in which to introduce the reforms, namely, whether to include the provisions in, for instance, a penal code, a cybercrime or cybersecurity law, a child rights or child protection law, an online safety or online harms law or a combination of these approaches.

There is not a *'one size fits all'* response to these questions and, indeed, there are examples of States taking one or several of these approaches.

Examples: **Australia, Fiji, Ghana, the Republic of the Philippines, United Kingdom of Great Britain and Northern Ireland, Zimbabwe**



In 2021, **Australia** passed the Online Safety Act updating its regulatory framework to give the eSafety Commissioner, Australia's online safety regulator, increased powers to tackle online harms, including online child sexual exploitation and abuse. The Act also establishes a set of core *'Basic Online Safety Expectations'* for the technology industry and gives the eSafety Commissioner the power to require companies to report on their implementation of the Expectations. The obligation to respond to a reporting requirement is enforceable and backed by civil penalties. The Commissioner can also issue statement to a provider of compliance and non-compliance with the Expectations.¹⁶⁷ This regulatory regime is discussed in more detail in **Part 7: Duties and responsibilities in relation to business** and **Part 10: Independent monitoring and regulation**.

In **Fiji**, the Online Safety Act 2018 established the Online Safety Commission to promote online safety and to receive and investigate complaints in relation to electronic communications that cause or intend to cause harm.

In **Ghana**, provisions relating to the criminalization and investigation of online child sexual exploitation and abuse were included in the Cybersecurity Act 2020.

In the **Philippines**, at the time of writing, consultations are underway on the draft Special Protections against Online Sexual Abuse and Exploitation of Children Law which contains provisions on the criminalization, prosecution and investigation of online child sexual exploitation and abuse as well as duties and obligations of the public and private sectors to protect children from online child sexual exploitation and abuse.

In the **UK**, at the time of writing, the Government has published an Online Safety Bill which establishes a regulatory framework for the private sector and imposes a duty on certain internet service providers to protect the public from online harms, including child sexual exploitation and abuse.

In **Zimbabwe**, provisions relating to the criminalization and investigation of online child sexual exploitation and abuse were included in the Data Protection Act No. 5 of 2021 which subsequently amended the Criminal Law (Codification and Reform) Act.

The approach taken will depend on a range of factors, which should be considered in the context of the jurisdiction in question. These include:

- The findings of a comparative analysis of the laws of the State against international and regional standards: A comparative analysis will highlight the strengths and gaps of the existing domestic legal framework and indicate the amendments which need to be made. If, for example, amendments are needed to criminal procedures to permit the collection, preservation, storage, sharing and admissibility of digital evidence, these amendments

may be more appropriately located in a cybersecurity law or criminal procedure code, particularly if these laws provide an existing framework for investigating cybercrimes. Similarly, if amendments are needed to ensure that child victims of online child sexual exploitation and abuse are referred to child protection authorities when they are in need of care and protection, amendments are more likely to be more appropriately located in national child protection legislation, such as a children's act, child rights law or similar legislation. Alternatively, if the legislative reforms relate to the regulation of industry and their duties or responsibilities to protect the public from online harms, this may provide opportunities to incorporate provisions relating to the protection of children from online child sexual exploitation and abuse.

- Existence of strategic partnerships: The existence of strategic partnerships within government may heavily influence the approach taken to the legislative reforms. If, for example, the ministry or department responsible for communications is leading the calls for legislative reform, the legal amendments may be more easily introduced in legislation led by that ministry/department, such as a cybersecurity or cybercrime law (see, for example, the Ghana case study below).
- Opportunities for advocacy in ongoing legal reforms: Ongoing legislative reform efforts that may not have children as a focus or prime motivation can nevertheless provide opportunities to incorporate provisions to protect children from online child sexual exploitation and abuse (see, for example, the Zimbabwe case study below).
- Accessibility: A separate law, for example, on online safety or cybercrime law, may be more accessible and easier to use by professionals and the public, than if the amendments are scattered in the criminal code and children's law, though this may not always be the case depending on the existing legal framework in the State or jurisdiction.

Example: Ghana

As explored in **Part 4: Stakeholder engagement and catalysts for legal reform** the inclusion of legal amendments relating to online child sexual exploitation and abuse in the Cybersecurity Bill (as opposed to the Children’s Bill) had several advantages in terms of strengthened multi-sectoral engagement and consultation, particularly with the telecommunications and private sectors. This approach also had a benefit for child rights advocates: they were able to advocate for amendments to other, more general provisions of the Cybersecurity Bill, which they would not have been able to do if they had not been formally involved in the consultation process.¹⁶⁸ For example, as a formal stakeholder in the consultation process, UNICEF and partners succeeded in advocating for the inclusion of ‘*child protection*’ as a grounds for the courts to order a service provider to block, filter and take down illegal content enshrined in Article 87 of the Cybersecurity Law.¹⁶⁹

Example: Zimbabwe

In Zimbabwe, calls for strengthening data protection laws provided opportunities for child rights advocates to strengthen the law to protect children from online child sexual exploitation and abuse.¹⁷⁰ Though the initial focus of the consultations on the then draft Cybersecurity and Data Protection Bill was on data protection and cybercrime more broadly, UNICEF and civil society advocated for the inclusion of specific provisions to protect children from online harm and to introduce offences relating to child sexual abuse material as a distinct issue from pornography; online solicitation of children for sexual purposes and sexual exploitation of children in the context of travel and tourism.¹⁷¹ The law, which was adopted as the Data Protection Act No. 5/2021, introduced new provisions in Zimbabwe’s Criminal Law (Codification and Reform) Act criminalizing certain forms of online child sexual exploitation and abuse. These included a new Article 165A(1)-(2) on child sexual abuse material, Article 165A(3) on ‘*cybergrooming*’, reflecting Article 23 of the Lanzarote Convention,¹⁷² and Article 165B on exposing children to pornography.

Consequential amendments to other laws **should** be identified

Regardless of the approach taken, any new law is likely to require amendments to other, already existing laws. These include possible amendments to provisions concerning the classification of film, videos and publications.

Endnotes

167 For a summary of the Online Safety Act 2021, please see the Fact Sheet produced by the eSafety Commissioner at www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf, accessed 28 March 2022.

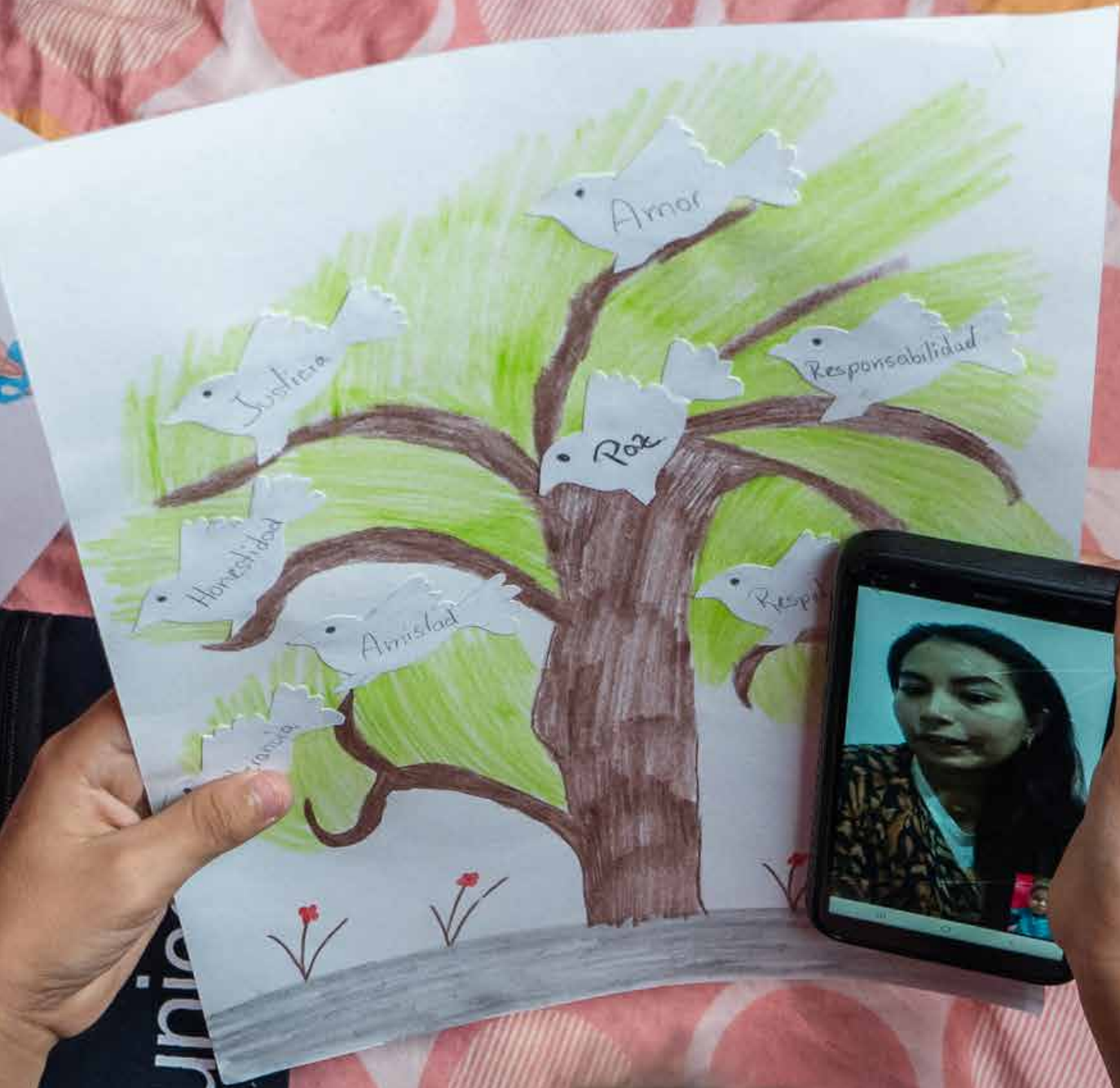
168 Online individual interview, UNICEF Ghana, 29 September 2021.

169 Ibid.

170 Online individual interview, NGO representative in Zimbabwe, 28 March 2022.

171 Ibid.

172 Article 23 of the Lanzarote Convention requires States parties to criminalize the solicitation of children for sexual purposes, i.e., the ‘intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2 [the age of sexual consent], for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a [engaging in sexual activities with a child who has not reached the age of sexual consent under the national law], or Article 20, paragraph 1.a [production of child pornography, as this term is defined in the Convention], against him or her, where this proposal has been followed by material acts leading to such a meeting’.



6. Criminalization of online child sexual exploitation and abuse

Checklist of minimum and recommended standards

Ensure that a child is defined as any person under the age of 18 years

Ensure the inclusion of a comprehensive definition of sexual abuse and exploitation of children, including where it is facilitated with the use of ICTs

Ensure that presumed consent by the child to the abuse or exploitation is null and void

Adolescents who are close in age, maturity and development **should not** be criminalized for consensual and non-exploitative sexual activity, provided that there is no element of coercion, abuse of trust or dependency between the adolescents, regardless of whether or not it is facilitated by the use of ICTs

Ensure that the law includes specific crimes relating to producing, offering, distributing, disseminating, importing, exporting, interacting with, accessing, possessing, and producing or disseminating material to advertise, child sexual abuse material, including live-streaming of child sexual abuse

A child **should not** be held criminally liable for the generation, possession, or voluntary and consensual sharing of sexual content of him/herself, solely for own private use, but instead States **should**:

- Establish clear legal frameworks that protect children and
- Through prevention efforts, ensure that children are educated about and made aware of the gravity of spreading content of others and of oneself

Sexual extortion of children **should** be criminalized, regardless of whether or not it is facilitated by the use of ICTs

Grooming of children **should** be criminalized, regardless of whether or not it is facilitated by the use of ICTs

Ensure the criminalization of attempts, complicity and participation in offences contained within the OPSC and consider criminalizing attempts, complicity and participation in other online child sexual exploitation and abuse offences

Consider including a specific offence of intentionally causing a child, for sexual purposes, to witness sexual abuse or sexual activities through the use of information and communication technologies, including where the child is not required to participate (subject to the standards above on self-generated sexual content)

Consider including other specific crimes relating to online child sexual exploitation and abuse, such as 'cyberflashing' or 'cyberstalking'

Consider introducing universal jurisdiction for all offences of child sexual exploitation and abuse, irrespective of whether or not they are facilitated with the use of information and communication technologies, and removing any requirement for 'double criminality' for such offences

Child sexual exploitation and abuse offences **should** be recognized by law as extraditable offences, regardless of whether or not they are facilitated by the use of information and communication technologies

- Extradition **should not** be conditional upon the existence of an extradition treaty with the other concerned State(s)

Law enforcement authorities **should** be required to take suitable measures to submit the case to its competent authorities for the purpose of prosecution in the event that the alleged perpetrator is not extradited on the basis of the alleged perpetrator's nationality

The statute of limitations in respect of offences of child sexual exploitation and abuse, irrespective of whether or not it is facilitated by the use of information and communication technologies, **should** be removed

Ensure minimum penalties/sanctions for adult perpetrators and enhanced penalties/sanctions for aggravating factors including young age of the victim

Ensure that children alleged as, accused or convicted of a crime, including of online child sexual exploitation and abuse offences, are handled within a separate child justice system in accordance with child-friendly justice principles and procedures

6.1 International law and guidance

Under Article 34 of the CRC, States parties have an obligation to protect children from all forms of sexual exploitation and abuse. In doing so, States parties must *'in particular take all appropriate national, bilateral and multilateral measures'* to prevent the inducement or coercion of a child to engage in any unlawful sexual activity, the exploitative use of children in prostitution or other unlawful sexual practices, and the exploitative use of children in pornographic performances and materials.¹⁷³

The criminalization of online sexual exploitation and abuse forms part of a State party's obligations to protect children under Article 34 of the CRC. In General Comment No. 25 (2021), the CRC Committee affirms this by calling upon States parties to put *'appropriate legislation'* in place *'to protect children from the crimes that occur in the digital environment'* and *'to allocate sufficient resources to ensure that crimes in the digital environment are investigated and prosecuted'*,¹⁷⁴ which includes online child sexual exploitation and abuse offences. Similarly, in the OPSC Guidelines, the CRC Committee recommends that States parties should assess their national legal and policy frameworks to ensure that they adequately cover *'all manifestations of the sale, sexual exploitation and sexual abuse of children, including when these offences are committed or facilitated through ICT'*.¹⁷⁵

The OPSC details States parties' obligations to criminalize particular forms of sexual exploitation and abuse, namely the sale of children, *'child prostitution'* and *'child pornography'*.¹⁷⁶ Article 3 of the OPSC requires States parties to ensure, *'as a minimum'*, that certain acts and activities are criminalized, regardless of whether they are carried out domestically or transnationally, or on an individual or organized basis. These acts include:

- In the context of the sale of children, offering, delivering or accepting, by whatever means, a child for the purpose of sexual exploitation of the child or engagement in forced labour;
- *'Offering, obtaining, procuring or providing a child for child prostitution'*; and
- *'Producing, distributing, disseminating, importing, exporting, offering, selling or possessing... child pornography'* for the purposes of sexual exploitation.¹⁷⁷

The OPSC also requires States parties, subject to the provisions of their national laws, to criminalize attempts of, and complicity or participation in, the acts listed above.¹⁷⁸

The OPSC Guidelines make it clear that OPSC offences should be interpreted to include online manifestations of these forms of violence. This interpretation aligns with one of the key aims

of the OPSC Guidelines, which is to ensure that the OPSC *‘remains an instrument that enhances the protection of children from sale and sexual exploitation, whether such offences are facilitated by ICT or not’*.¹⁷⁹ Relevant guidance from the

OPSC Guidelines in relation to specific offences and minimum standards is highlighted as relevant throughout this **part 6: Criminalization of online child sexual exploitation and abuse**.

6.2 Regional law and guidance

Regional laws affirm States parties’ obligations to criminalize online sexual exploitation and abuse. These include Article 27 of the ACRWC, which requires States parties to protect children from *‘all forms of sexual exploitation and sexual abuse’* including the inducement, coercion or encouragement of a child to engage in any sexual activity, the use of children in prostitution or other sexual practices and the use of children in pornographic activities, performances and materials. In its General Comment No. 7 (2021), ACRWC Committee affirms that Article 27 should be interpreted to include online and offline sexual exploitation and abuse and provides detailed guidance for States parties on criminalizing these forms of violence. The ACRWC Committee also highlights the challenge of new and emerging forms of online sexual exploitation and abuse, which requires that *‘both substantive criminal law and investigative and evidence collection techniques be developed to accommodate them’*.¹⁸⁰

States parties to the Budapest Convention, which is the Council of Europe’s main cybercrime convention, are required to criminalize certain conduct relating to cyberspace, including various offences related to *‘child pornography’* (as it is referred to in the Convention).¹⁸¹ The Lanzarote Convention, which is the Council of Europe’s convention on protecting children from sexual exploitation and abuse, also requires States parties to criminalize online and offline sexual exploitation and abuse of children, as well as aiding, abetting and attempts to commit such crimes.¹⁸²

Within the framework of the European Union, Directive 2011/93 on Combating Child Sexual Exploitation and Abuse requires Member States

to take necessary measures to ensure that sexual abuse and exploitation is punishable.¹⁸³

There are also various other regional standards and model laws which require or recommend the criminalization of certain means and manifestations of online sexual exploitation and abuse. These instruments include:

- The African Union Convention on Cyber Security and Personal Data Protection (which has not yet entered into force); the Economic Community of West African State’s Directive C/DIR 1/08/11 on Fighting Cyber Crime; the Southern African Development Community Model Law on Computer Crime and Cybercrime; and the East African Community Framework for Cyberlaws;
- The Arab Convention on Combating Information Technology Offences;
- The Model Policy Guidelines and Legislative Texts on cybercrime and e-crime developed by Caribbean Community and a group of African, Caribbean and Pacific States, the International Telecommunications Union, among others;¹⁸⁴ and
- The Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN and Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN.

Relevant provisions from these instruments are highlighted where relevant throughout this part.

6.3 Detail of minimum and recommended standards

Ensure that a child is defined as any person under the age of 18 years

Under international and regional standards, a child is any person under the age of 18 years.¹⁸⁵ The sexual abuse and exploitation of all children, both boys and girls, up to 18 years, should be criminalized.¹⁸⁶

Ensure the inclusion of a comprehensive definition of sexual abuse and exploitation of children, including where it is facilitated with the use of ICTs

Though it falls outside the scope of this Global Guide to provide detailed guidance on provisions relating to sexual abuse and exploitation of children more generally, the drafting of crimes of online sexual exploitation and abuse of children are often linked to generic provisions on sexual exploitation and abuse of children. This situation may arise where the law of a State contains existing provisions and definitions of *'sexual abuse and exploitation'*, which are in turn used to draft more specific definitions for the crimes of online sexual exploitation and abuse. To ensure that the online crimes are comprehensive in scope, it is therefore necessary to review and consider whether existing generic definitions are similarly in line with international child rights standards and capture online and offline means and manifestations of child sexual exploitation and abuse.

The formulation of the definitions and crimes will vary by State. However, the definitions of child sexual abuse and exploitation, including online child sexual abuse and exploitation, in **Part 1.6** of this Global Guide on definitions and terminology, which are based primarily on the Luxembourg Guidelines, should inform the drafting of the definitions of the crimes of child sexual exploitation and abuse and online child sexual exploitation and abuse in the law.

Although this Global Guide provides standalone descriptions of online child sexual exploitation and abuse, it is important to recall that the boundary

between online and offline sexual exploitation and abuse in practice is often blurred.¹⁸⁷

✓ This challenge reinforces the importance of reviewing generic definitions of crimes relating to sexual exploitation and abuse to ensure that they capture all forms of sexual exploitation and abuse of children committed with or without the use of ICTs.

✓ Following the approach of the Council of Europe's Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, when drafting definitions of online child sexual exploitation and abuse, it is important to ensure that the terms are *'where possible formulated in a technology-neutral manner, leaving room for the emergence of new technologies'*.¹⁸⁸

Ensure that presumed consent by the child to the abuse or exploitation is null and void

Children cannot be regarded as consenting to their abuse or exploitation. Any provisions which provide exemptions, justifications or defences based on a child's presumed 'consent' to their abuse or exploitation, whether or not it is facilitated by the use of ICTs, must therefore be removed from the law. Consideration may also be made to adding a provision to the law indicating that any such presumed consent by the child to the abuse or exploitation shall be null and void for the purposes

of determining whether a crime against the child has been committed.¹⁸⁹ However, as explained below, consensual sexual activity between adolescents who are close in age, maturity and development, with no element of coercion, abuse of trust or dependency between the participants, should not in itself be regarded as abusive or exploitative, and therefore should not fall within the scope of any such provisions which render the consent null and void.

Adolescents who are close in age, maturity and development **should not** be criminalized for consensual and non-exploitative sexual activity, provided that there is no element of coercion, abuse of trust or dependency between the adolescents, regardless of whether or not it is facilitated by the use of ICTs

National laws often criminalize sexual activity with a child under the age of sexual consent, regardless of whether the sexual activity appears consensual on the part of the child. Although international standards recommend that States prescribe a minimum age of sexual consent in their law,¹⁹⁰ there is little international consensus on the age for sexual consent.¹⁹¹ The CRC Committee has acknowledged this gap, as it has recommended that States parties should 'take into account the need to balance protection and evolving capacities and define an acceptable minimum age when determining the legal age for sexual consent'.¹⁹²

Discussions relating to the minimum age of consent are likely to arise when States seek to set out definitions of the crimes of online sexual abuse and exploitation in law, particularly in relation to consensual sexual activity between adolescents where one, or both, of the adolescents are under the age of sexual consent.

In 2011, the CRC Committee made a distinction between i) sexual activity 'imposed' by an adult on a child 'where the child is entitled to protection by criminal law', ii) sexual activity committed by a child against another child where there is a significant difference in age or use of 'power, threat or other

means of pressure', and iii) sexual activity between children older than the age of sexual consent. According to the CRC Committee, the former two acts constitute sexual abuse, while the latter does not.¹⁹³ In General Comment No. 20 (2016), the CRC Committee elaborated on its guidance and recommended, without reference to the minimum age of consent, that, 'States should avoid criminalizing adolescents of similar ages for factually consensual and non-exploitative sexual activity'.¹⁹⁴ The CRC Committee reiterates this guidance in the OPSC Guidelines, by recommending that, 'States parties should not criminalize adolescents of similar ages for consensual sexual activity'.¹⁹⁵ These recommendations should be interpreted as applying to all sexual activity, regardless of whether or not it is facilitated by the use of ICTs.

Regional standards generally echo the CRC Committee's recommendations. The ACRWC Committee recommends that States parties to the ACRWC 'should decriminalize consensual, non-abusive and non-exploitative sexual activities among child peers'.¹⁹⁶ This recommendation should be interpreted as applying to all such consensual, non-abusive and non-exploitative sexual activity among child peers, regardless of whether or not it is facilitated by the use of ICTs.¹⁹⁷

In the EU, Member States have an element of discretion over the criminalization of peer-to-peer sexual activity. EU Directive 2011/93 on Combating Child Sexual Exploitation and Abuse explicitly does not cover Member States' policies with regard to *'consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development, taking account of the different cultural and legal traditions and of new forms of establishing and maintaining relations among children and adolescents, including through information and communication technologies'*.¹⁹⁸ Article 8 on *'consensual sexual activities'* provides that Member States have discretion in deciding whether or not the following crimes apply to *'consensual sexual activities between peers who are close in age and degree of psychological and physical development or maturity, in so far as the acts did not involve any abuse'*:

- Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual activities, even without having to participate; and
- Engaging in sexual activities with a child who has not reached the age of sexual consent.

✓ This is a complex issue that requires careful consultation and drafting.

The rationale for decriminalizing sexual activity between consenting adolescents who are close in age, irrespective of whether or not it is facilitated by the use of ICTs, is based on a recognition of the evolving capacities of the child and that the activity does not have the nature of abuse or exploitation. Criminalization also exposes children to the potentially harmful and stigmatizing effects that coming into conflict with the law entails¹⁹⁹ and does not necessarily prevent children from engaging in sexual activity.²⁰⁰ The ACRWC Committee explains that there is a risk that criminalization drives the activity *'underground'* and can create barriers to children accessing education and sexual and reproductive health services, leading to *'higher unsafe abortion rates, STDs [sexually-transmitted diseases] and unwanted pregnancies'*.²⁰¹ The exception is conditional, however, on the

adolescents giving informed consent and there being no element of coercion or abuse of trust or dependency between the participants. In addition, it is important to acknowledge that sexual activity which is initially consensual may subsequently become abusive or exploitative. This may arise, for example, when an adolescent voluntarily and consensually shares a sexual content of him/herself, but that image or video is subsequently shared beyond the control of the adolescent who created it²⁰² (see below for the standards on **self-generated sexual material** by children). Further, as highlighted by the ACRWC Committee, it is important that adolescents have access to sexual and reproductive information and services to be able to make informed decisions on their sexual behaviour.²⁰³

To address these issues in legislation, States have introduced what is colloquially referred to as *'close-in-age,' 'age-gap' or 'Romeo and Juliet clauses'*.²⁰⁴ These provisions decriminalize consensual sexual activity among adolescents provided that they fall within a stipulated age frame, which varies from State to State, but which is reportedly no more than five years.²⁰⁵

When legislating for online sexual abuse and exploitation, stakeholders should therefore incorporate a *'close-in-age exception'* or defence to criminal charges for consensual online sexual activity between adolescents who are close in age, maturity and development, provided that there is no relationship of trust, authority or dependency between the participants.²⁰⁶ Such debates are likely to involve a reflection on how consensual sexual activity between adolescents is handled more generally under the criminal law, not just in relation to the digital environment, and should therefore be approached with careful consideration in light of the context in the State.

In any event, children coming into conflict with the law should always be treated in accordance with child justice standards, including the availability of pre-trial diversion mechanisms and the purpose of rehabilitating rather than punishing the child (see further below for **standards on child-friendly justice**).

Ensure that the law includes specific crimes relating to producing, offering, distributing, disseminating, importing, exporting, interacting with, accessing, possessing, and producing or disseminating material to advertise, child sexual abuse material

Article 2 of the OPSC defines ‘*child pornography*’ as ‘*any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child for primarily sexual purposes*’.²⁰⁷ However, as recommended by the CRC Committee and Luxembourg Guidelines, the term ‘*child pornography*’ should be avoided to the extent possible and replaced by terms such as ‘*child sexual abuse material*’;²⁰⁸ which is the approach taken in this Global Guide. The main reason for this approach is that the term ‘*pornography*’ does not appropriately reflect the abusive aspect of the issue and risks undermining its severity.²⁰⁹

Under international standards, legislation concerning child sexual abuse material should be introduced or amended to incorporate technology-specific terminology and specifically capture child sexual abuse material available online.²¹⁰ This guidance was made clear in the OPSC Guidelines, in which the CRC Committee recommends that,

- The phrase, ‘*by whatever means*’ in Article 2 of the OPSC should be interpreted to include the ‘*broad range of material available in a variety of media, both online and offline*’;²¹¹
- The phrase, ‘*simulated explicit sexual activities*’ in Article 2 of the OPSC should be interpreted to include ‘*any material, online or offline, that depicts or otherwise represents a child appearing to engage in sexually explicit conduct*’.²¹²

Child sexual abuse material includes live performances and, arguably, computer-generated child sexual abuse material’;²¹³ which are ‘*images that have been created with the purpose of conveying the impression that they depict children*’.²¹⁴

Similar definitions of child sexual abuse material are provided in regional instruments, a comprehensive overview of which is available in the Luxembourg Guidelines.²¹⁵

In addition to ensuring that the definition of child sexual abuse material includes both online and offline components, so too should crimes relating to their production, possession and use. This point is emphasized in the Luxembourg Guidelines, which provide that, in order to combat this problem, it is necessary to ‘*attach a criminal consequence to the conduct of each participant in the chain, from production to possession/consumption*’.²¹⁶

✓ Based on CRC Committee recommendations and the ICMEC model legislation on combating child sexual abuse material, at a minimum, legislation should therefore criminalize the following acts/ omissions, including specifically where such acts are carried out online or facilitated with the use of ICTs:

- Production of child sexual abuse material;
- Offering child sexual abuse material;
- Distribution or dissemination of child sexual abuse material;
- Importing or exporting of child sexual abuse material;
- Interacting with child sexual abuse material online, for example, by commenting on photographs, sharing comments using the chat or ‘*comments*’ functions, or sending instructions, encouragement or direction remotely;
- Accessing child sexual abuse material, including both live and pre-recorded displays, acts or performances;
- Possession of child sexual abuse material regardless of the intent to distribute, subject to exceptions based on legitimate professional requirements, such as by law enforcement for the purposes of investigation and prosecution of crimes; and
- Production or dissemination of material advertising child sexual abuse or exploitation or making known to others where to find child sexual abuse material.²¹⁷

Example: Ghana



Article 62 of the Cybersecurity Act 2020 criminalizes acts relating to child sexual abuse material (defined in the Act as ‘*indecent images or photographs of a child*’). An extract is provided below.

‘Indecent image or photograph of a child

62. (1) A person shall not

(a) take or permit to be taken an indecent image or photograph of a child;

(b) produce or procure an indecent image or photograph of a child for the purpose of the publication of the indecent image or photograph through a computer system;

(c) publish, stream, including live stream, an indecent image or photograph of a child through a computer or an electronic device; or

(d) possess an indecent image or photograph of a child in a computer system or on a computer or electronic record storage medium.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not less than 2,500 penalty units and not more than 5,000 penalty units or to a term of imprisonment of not less than 5 years and not more than 10 years or to both.

(3) For purposes of paragraph (c) of subsection (1), a person publishes an indecent photograph, image or visual recording if that person,

(a) parts with possession of the indecent photograph, image or recording to another person; or

(b) exposes or offers the indecent photograph, image or recording for acquisition by another person.

(4) For the purpose of this Section, “indecent image or photograph” includes a material image,

visual recording, video, drawing or text that depicts

(a) a child engaged in sexually explicit or suggestive conduct;

(b) a person who appears to be a child engaged in sexually explicit or suggestive conduct;

(c) images representing a child engaged in sexually explicit or suggestive conduct;

(d) sexually explicit images of children;

(e) any written material, visual representation or audio recording that advocates or counsels sexual activity with children that would be an offence under the Criminal Offences Act, 1960 (Act 29) or any other relevant enactment;

(f) any written material that has, as its dominant characteristic, the description, for a sexual purpose, of sexual activity with a child that would be an offence under the Criminal Offences Act, 1960 (Act 29) or any other relevant enactment; or

(g) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a child that would be an offence under the Criminal Offences Act, 1960 (Act 29) or any other relevant enactment.’

‘Interpretation

97. In this Act, unless the context otherwise requires,

.....

“child” means a person below the age of 18 years;

.....

“computer” means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic or storage functions, and includes any data storage facility

or communications facility directly related to or operating in conjunction with such device;

.....

“computer system” means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes

an information system; and

an operational technology system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system.’

(c) distributes or transmits child sexual abuse material;

(d) procures or obtains child sexual abuse material for oneself or for another person;

(e) possesses child sexual abuse material on a computer system or a computer-data storage medium;

(f) knowingly obtains, accesses or procures child sexual abuse material;

(g) baits a child into the production or distribution of child sexual abuse material;

shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding 10 years, or both such fine and such imprisonment.

.....’

Example: Zimbabwe



Zimbabwe’s Data Protection Act No.5/2021 introduced new Section 165A to the Criminal Law (Codification and Reform Act) to criminalize certain acts relating to child sexual abuse material, as follows:

‘165A Child sexual abuse material

(1) In this Act—

“Child sexual abuse material” means any representation through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a child, a person made to appear as a child or realistic material representing a child, engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a child for primarily sexual purposes.

(2) Any person who unlawfully and intentionally, through a computer or information system—

(a) produces child sexual abuse material;

(b) offers or makes available child sexual abuse material;

A child **should not** be held criminally liable for the generation, possession, or voluntary and consensual sharing of sexual content of him/herself, solely for own private use, but instead States **should**:

- Establish clear legal frameworks that protect children and
- Through prevention efforts, ensure that children are educated about and made aware of the gravity of spreading content of others and of oneself

When legislating for the criminalization of child sexual abuse materials, challenges may arise regarding what is often referred to as ‘*self-generated sexual content*’ and ‘*sexting*’.



Self-generated sexual content refers to sexual content generated by the child him/herself.²¹⁸

‘*Sexting*’ is frequently used to describe self-generated sexual content sent via mobile phone text messaging or other online messaging to others.²¹⁹

The Committee of the Parties to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Committee) has stated that children may ‘*explore and express their sexuality through ICTs, including by generating and sharing sexually suggestive or explicit images and/or videos of themselves*’.²²⁰ The Lanzarote Committee has highlighted that the aim of such ‘*voluntary and consensual sharing*’ of self-generated sexual content by children is not to distribute sexual abuse material.²²¹ However, a child’s understanding of the consequences of sharing the content varies according to their age and maturity, such that the child may not be fully aware of the risks that sharing the material entail.²²²

Risks to the child include the distribution of such material by others. Once shared, the content may be spread online or offline beyond the child’s control or against the child’s wishes and can be difficult to remove or take down. It can also be used to bully the child, as a mechanism for sexual extortion and for sexual grooming, which can have serious and traumatizing consequences for the child.²²³



The term ‘*self-generated*’ sexual content has been criticized for implying that the child is partly to blame for the abuse or exploitation that was involved in its generation, or which ensues from the content being distributed online.²²⁴ This has led to the proposal of alternative terms such ‘*first person produced imagery*’.²²⁵ At the time of writing, an alternative term to describe such acts has yet to be agreed under international standards. This Global Guide therefore uses the term ‘*self-generated sexual content*’ with the clarification that the use of this term is not intended to impose any degree of blame or responsibility on the victim for any abuse or exploitation they experience in connection with the content.

International standards

In light of the above, the CRC Committee recommends that ‘*self-generated sexual material by children that they possess and/or share with their consent and solely for their own private use should not be criminalized*’.²²⁶ Instead, the CRC Committee recommends that ‘*child-friendly channels should be created to allow children to safely seek advice and assistance where it relates to self-generated sexually explicit content*’.²²⁷ While the CRC Committee does not elaborate on the types of ‘*advice and assistance*’, as the statement is within a section of the General Comment concerning the administration of child justice, it is presumed to relate to advice and assistance on children’s legal rights and remedies, reporting channels for notice and takedown and other assistance that should be made available to support child victims (for which see **Part 9: Victim support, rehabilitation, reintegration and redress**).

Similarly, the OPSC Guidelines provide that a distinction must be made between ‘*child pornography*’ (i.e. child sexual abuse material), which constitutes a criminal offence, and ‘*the production by children of self-generated sexual content or material representing themselves*’.²²⁸ The CRC Committee’s concern is that the self-generated aspect of such content could increase the risk that the child is considered responsible instead of being treated as a victim, and therefore ‘*underscores that children should not be held criminally liable for producing images of themselves*’.²²⁹ The CRC Committee states that this issue requires ‘*careful attention*’ by States parties, which should ‘*establish clear legal frameworks that protect children and, through prevention efforts, ensure that they are educated about and made aware of the gravity of spreading images of others and of oneself*’²³⁰ (see **Part 11: Implementation of legislation**).

Regional standards

Regional standards provide similar guidance to States parties concerning self-generated sexual content by children. The ACRWC Committee echoes the CRC Committee and provides that children ‘*should never face criminal liability for their role in producing or making available the material depicting themselves*’.²³¹ The ACRWC Committee also recommends that images made by children consensually, for private use, should not constitute child sexual abuse material, ‘*unless such images are produced as a result of coercion, blackmailing or other forms of undue pressure against the will of the child*’.²³² However, where such coercion, blackmail or undue pressure exists, the child who created the material should not be prosecuted.²³³

The Lanzarote Committee provides similar guidance in its opinion on ‘*child sexually suggestive or explicit images and/or videos generated, shared and received by children*’ adopted in 2019. If the child in question is ‘*in a particularly vulnerable situation*’ (for example, a very young or prepubescent child, a child with disabilities or child in a situation of dependence), the content should be considered ‘*the result of abusive/exploitative conduct*’ such that the child should be referred to victim support and not subject to criminal prosecution.²³⁴ Similarly,

children whose self-generated content is ‘*exploited (offered or made available, distributed or transmitted to others)*’ should be referred for victim support and not subject to criminal prosecution.²³⁵

The Lanzarote Committee provides that ‘*the self-generation of sexually suggestive or explicit images and/or videos by children does not amount to the “production of child pornography” when it is intended solely for their own private use*’.²³⁶ Similarly, the ‘*possession by children of sexually suggestive or explicit images and/or videos of themselves does not amount to “the possession of child pornography” when it is intended solely for their own private use*’.²³⁷ Further, the ‘*voluntary and consensual sharing by children among each other of sexually suggestive or explicit images and/or videos of themselves does not amount to “offering or making available, distributing or transmitting, procuring, or knowingly obtaining access to child pornography” when it is intended solely for their own private use*’ (emphasis added).²³⁸ The element of consent for the sharing of the images between the parties is significant as it implies that, where child A does not voluntarily and consensually receive such images from child B, which may be the case if child B uses the images to sexually harass child A, the guidance against criminalization of child B does not apply (though the child must be treated in accordance with child justice principles, for which see below for **standards on child-friendly justice**).²³⁹

The Lanzarote Committee issued additional guidance in 2022, noting that conduct related to self-generated sexual content may fall within the scope of other provisions of the Lanzarote Convention, such as Article 18 on sexual abuse, Article 19 relating to offences concerning child prostitution and, among other things, include extortion of children for sexual, financial or other gain.²⁴⁰ However, the Lanzarote Committee provides that children are victims ‘*and should thus be treated as such and not be subject to criminal prosecution*’.²⁴¹ It goes on to:

- Recommend that States parties ‘*should consider introducing an explicit reference to such self-generated materials in their legislation as far as*

offences covered by the Lanzarote Convention are concerned’;

- Invite States parties ‘to strengthen the protection of children by introducing explicit references in their respective legal frameworks to conduct concerning child self-generated sexual images and/or videos, identifying the circumstances when children should not be held criminally liable and when they should be prosecuted only as a last resort’;
- Request States parties to ensure in their legal frameworks that a child will not be prosecuted when he/she possesses ‘their own self-generated suggestive or explicit images and/or videos’, or those of another child with the informed consent of the child depicted on them or as a result of receiving them passively without asking for them; and
- Request States parties to ensure in their legal framework that a child will not be prosecuted for sharing his/her sexual images and/or videos with another child when such sharing is voluntary, consensual and intended solely for their own private use.²⁴²

In similar vein, Article 8 of EU Directive 2011/93 on Combating Child Sexual Exploitation and Abuse provides EU Member States with the discretion to decide whether the offences of knowingly attending pornographic performances involving the participation of a child apply in the context of ‘a consensual relationship where the child has reached the age of sexual consent or between peers who are close in age and degree of psychological and physical development or maturity, in so far as the acts did not involve any abuse or exploitation and no money or other form of remuneration or consideration is given as payment in exchange for the pornographic performance’.²⁴³ Similarly, Member States have the discretion to decide whether offences relating to the production, acquisition or possession of child pornography²⁴⁴ apply to ‘material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse’.²⁴⁵

✓ In sum, legislation should therefore, at a minimum, include a provision confirming that a

child shall not be brought into conflict with the law for self-generating, possessing or voluntarily and consensually sharing sexual material of him/herself solely for private use. At the same time, preventative educative measures should inform children about safe online conduct and the risks involved in sharing self-generated material (see **Part 11: Implementation of legislation**), or the making of child protection referrals where appropriate (see **Part 8: Procedures and methods of investigation of online child sexual exploitation and abuse**).

Example: England and Wales

This case study provides an example of the challenges that can arise in the absence of legislative exemptions to the criminalization of children who generate, possess or voluntarily and consensually share sexual images of themselves for private, non-abusive and non-exploitative purposes and possible ways of addressing this pending legislative reform.

Offences relating to child sexual abuse material, or ‘indecent images of children’ as it is referred to in England and Wales, are set out in Section 1 of the Protection of Children Act 1978 and Section 160 of the Criminal Justice Act 1988. These provisions, which were drafted before internet access and smart phones became commonplace, do not incorporate any exceptions for the creation, possession or voluntary and consensual sharing of self-generated sexual material by a child. Consequently, a child who makes, possesses, shares or shows any indecent images of him/herself may be prosecuted under these laws.

Recognizing the inflexibility of the law and the disproportionate criminalization of children for ‘sexting’, in 2016, the UK Home Office introduced ‘Outcome 21’ to the Home Office Counting Rules²⁴⁶ which provide police forces with the following option to record the offence: ‘Further investigation, resulting from the crime report, which could provide evidence sufficient to support formal action being taken against the named suspect, is not in the public interest – police decision’.²⁴⁷ Outcome 21 in effect allows police forces to record the crime as having taken place

but that no formal criminal justice action was taken as it was not considered to be in the public interest.²⁴⁸

The College of Policing provides that Outcome 21 *'may be considered the most appropriate resolution in youth produced sexual imagery cases where the making and sharing is considered non-abusive and there is no evidence of exploitation, grooming, profit motive, malicious intent (e.g. extensive or inappropriate sharing (e.g. uploading onto a pornographic website) or it being persistent behaviour'*.²⁴⁹ However, where these factors are present, Outcome 21 would not apply.²⁵⁰ Despite the introduction of Outcome 21, there is no guarantee that the crime will not be disclosed on the child's criminal background check in the future,²⁵¹ which may be regarded as defeating the purpose of the initiative.²⁵²

Despite this pragmatic effort to adapt the law to the realities of technological developments, an inquiry by the All-Party Parliamentary Group on Social Media and UK Safer Internet Centre found that Outcome 21 is applied inconsistently across England and Wales due to the wide scope of police discretion and uncertainty as to what is considered acceptable.²⁵³

Under international and regional standards, child recipients of self-generated sexual content by other children may be prosecuted for offences relating to child sexual abuse material in certain circumstances provided that the child is handled in the child justice system according to child-friendly justice principles (see further below on the **child justice system**). These circumstances include the following:

- The child coerces, blackmails or otherwise places undue pressure on another child to produce or share self-generated sexual content;
- The child, with knowledge and intention, procures or obtains access to self-generated sexual content by another child beyond or without the volition and consent of the child who is the subject of the material;

- The child shares (for example, distributes, disseminates, exports, offers or sells) self-generated sexual content of another child.

The OPSC Guidelines affirm that, if self-generated sexual *'images'* are produced as a result of *'coercion, blackmailing or other forms of undue pressure against the will of the child, those who made the child produce such content should be brought to justice'*.²⁵⁴ Further, if the self-generated *'images'* are subsequently *'distributed, disseminated, imported, exported, offered or sold as child sexual abuse materials, those responsible for such acts should also be held criminally liable'*.²⁵⁵

The Lanzarote Committee has requested States parties to ensure that a child who distributes or transmits self-generated sexually explicit images and/or videos of other children is only prosecuted *'as a last resort'* when such images and/or videos qualify as *'child pornography'* in accordance with the Lanzarote Convention.²⁵⁶

This is a complex area, with international and regional standards aiming to strike a balance between the evolving capacities of the child and the protection of children from exploitation and abuse. In sum, as a general rule, children should not be prosecuted for offences related to self-generated sexual images. However, in the circumstances outlined above, prosecution may be permitted where other alternative measures are not appropriate, in line with international child justice standards (see further below on the minimum standards concerning the **child justice system**).

Consider including a specific offence of intentionally causing a child, for sexual purposes, to witness sexual abuse or sexual activities through the use of ICTs, including where the child is not required to participate (subject to the standards above on self-generated sexual content)

Exposure to pornography can harm children, particularly if the child is exposed at a young age. It can lead to poor mental health, attitudes of sexism and objectification, sexual violence, and attitudes that abusive and misogynistic acts, which may form part of pornographic content, is normal and acceptable.

The act of showing pornography to a child may also be carried out by perpetrators with the use of ICT as part of the grooming process to desensitize the child to sexual conduct and manipulate the child into sharing sexualized images of themselves. The receipt by children of non-consensual sexual content or *'unwanted sexting'* (see above for commentary on sexting) may include *'receiving unwanted sexually explicit photos, videos, or messages, for instance by known or unknown persons trying to make contact, put pressure on, or groom the child'*.²⁵⁷

Though not explicitly set out in the CRC, the CRC Committee *'encourages States parties to criminalize the intentional causing, for sexual purposes, of a child to witness sexual abuse or sexual activities, even without having to participate'*.²⁵⁸ The ACRWC Committee reiterates this in General Comment No. 7 on Article 27 of the African Charter on the Rights and Welfare of the Child.²⁵⁹ The ICMEC Model Law to combat online grooming of children for sexual purposes also calls for these acts to be criminalized.²⁶⁰

The Council of Europe framework sets a similar standard, though it relates solely to children under the age of sexual consent. Article 22 of the Lanzarote Convention sets out the crime of *'corruption of children'* and requires States parties to take the necessary legislative or other measures to criminalize the intentional causing, for sexual purposes, of a child who has not reached the age of sexual consent, to witness sexual abuse or sexual activities, even without having to participate.

Example: Zimbabwe



Zimbabwe's Data Protection Act

No.5/2021 introduced new Section 165B to the Criminal Law (Codification and Reform Act) to introduce the new crime of exposing children to pornography:

'165B. Exposing children to pornography

Any person who unlawfully and intentionally through a computer or information system—

- (a) makes pornographic material available to any child; or
- (b) facilitates access by any child to pornography or displays pornographic material to any child;

with or without the intention of lowering the child's inhibitions in relation to sexual activity or inducing the child to have sexual relations with that person;

shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.'

Sexual extortion of children **should** be criminalized, regardless of whether or not it is facilitated by the use of ICTs

The OPSC Guidelines provide that **sexual extortion of a child** occurs when *'a child is forced into agreeing to give sexual favours, money or other benefits under the threat of sexual material depicting the child being shared on, for example, social media'*.²⁶¹

The Luxembourg Guidelines similarly describe sexual extortion as *'the blackmailing of a person with the help of self-generated images of that person in order to extort sexual favours, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media)'*.²⁶²

Sexual extortion is a form of child sexual exploitation and abuse, which should be criminalized when committed with or without the use of ICTs.²⁶³ It is also specifically referred to in regional instruments.

The term *'sexual extortion'* should be used instead of the term *'sextortion'*, as the latter term does not convey the exploitative nature of the violence and *'risks trivialising a practice that can produce extremely serious consequences'*.²⁶⁴

Example: Association of Southeast Asian Nations



The minimum legal standards listed in Annex 3 of the Regional Plan of Action, which ASEAN Member States are encouraged to adopt, include the criminalization of conduct and introduction of penalties for *'unwanted sexting and sexual extortion'*.

Example: Ghana



The Cybersecurity Act (No. 1038), 2020 introduced a new crime of online sexual extortion:

'Sexual extortion

66. (1) A person shall not threaten to distribute by post, email, text, or transmit, by electronic means or otherwise, a private image or moving images of the other person engaged in sexually explicit conduct, with the specific intent to

(a) harass, threaten, coerce, intimidate or exert any undue influence on the person, especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or

(b) actually extort money or other consideration or compel the victim to engage in unwanted sexual activity.

(2) A person shall not threaten to distribute by post, email, text, or transmit, by electronic means or otherwise, an intimate image of a child engaged in sexually explicit conduct, with the specific intent to

(a) harass, threaten, coerce, or intimidate the person, especially with intent to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or

(b) actually extort money or other consideration or compel the victim to engage in unwanted sexual activity.

(3) For the purposes of subsections (1) and (2), an intimate image may include a depiction in a way that the genital or anal region of another person is bare or covered only by underwear; or the breasts below the top of the areola, which is either uncovered or clearly visible through clothing.

(4) A person who contravenes subsection (1) or (2) commits an offence and is liable on summary conviction to a term of imprisonment of not less

than ten years and not more than twenty-five years.'

See, however, below on **sanctions and penalties**.

Grooming of children **should** be criminalized, regardless of whether or not it is facilitated by the use of ICTs

Grooming of children, also referred to as '*the solicitation of children for sexual purposes*', is '*the process of establishing a relationship with a child either in person or through the use of ICT to facilitate online or offline sexual contact*'.²⁶⁵

International and regional standards make it clear that online grooming of children should be criminalized.²⁶⁶ ICMEC recommends that legislation should incorporate online grooming of children as a separate offence to grooming of children.²⁶⁷

The Luxembourg Guidelines provide that online grooming includes the following four key elements:

- a. Contacting a child;
- b. Through the use of ICTs;
- c. With the intent of luring or inciting the child;
- d. To engage in any sexual activity by any means, whether online or offline.²⁶⁸

The third element – that of intent – is particularly noteworthy. As long as the alleged perpetrator has this intent, it is not necessary for a physical meeting to take place or even be attempted in order to constitute a crime.²⁶⁹ ICMEC's Model Legislation on Combating the Grooming of Children for Sexual Purposes similarly provides that the offence should be wide enough to capture the whole process of online grooming, which in itself can be harmful and exploitative of children, and should not be dependent on the perpetrator actually having physical contact or attempting to meet with the child in person.²⁷⁰

Example: Argentina



Penal Code, Law 11.179

*'Article 131. Anyone who, by means of electronic communications, telecommunications or any other data transmission technology, contacts a minor, with the purpose of committing any crime against the sexual integrity of the minor, will be punished with imprisonment from six (6) months to four (4) years.'*²⁷¹

In this example, in line with international standards, it is not necessary for the perpetrator to actually commit the crime against the sexual integrity of the minor in order for the offence of online grooming to occur. Contact with the purpose of committing such crimes is sufficient.

As the formulation of the crime of online grooming is tied to the definition of '*crimes against the sexual integrity of the minor*', it is necessary to ensure that such crimes are sufficiently comprehensive in scope and capture the full range of sexual activities which perpetrators may try to solicit from children.

A similar approach to the example above of Argentina is taken in Ghana, which links the crime of online grooming with the solicitation of '*unlawful sexual conduct of or with any child, or the visual depiction of such conduct*'. Further, in this example, the crime captures communications with children and persons believed by the perpetrator to be a child. This approach means that even where the recipient of the messages is not a child, the perpetrator may be prosecuted if he/she believed that person to be a child.

Example: Ghana



Cybersecurity Act (No. 1038), 2020
Dealing with a child for purposes of sexual abuse

63. A person shall not use

- (a) a computer online service,
- (b) an internet service,
- (c) a local bulletin board service, or

(d) any other device capable of electronic data storage or transmission

to seduce, solicit, lure, groom or entice, or attempt to seduce, solicit, lure, groom or entice, a child or another person believed by the person to be a child, for the purpose of facilitating, encouraging, offering, or soliciting unlawful sexual conduct of or with any child, or the visual depiction of such conduct.

(2) A person who contravenes subsection (1), commits an offence and is liable on summary conviction to a term of imprisonment of not less than five years and not more than fifteen years.

Ensure the criminalization of attempts, complicity and participation in offences contained within the OPSC and consider criminalizing attempts, complicity and participation in other online child sexual exploitation and abuse offences

The OPSC requires States parties, subject to the provisions of their national laws, to criminalize attempts of, and complicity or participation in, OPSC offences.²⁷²

Regional frameworks recommend criminalizing attempts, complicity and participation in a broader

range of online child sexual exploitation and abuse offences. The ACRWC Committee provides that attempts, complicity and participation in the full range of offences covered by its General Comment No. 7 (which includes the full range of online child sexual exploitation and abuse offences) should be criminalized under the national law.²⁷³

Consider including other specific crimes relating to online child sexual exploitation and abuse, such as ‘cyberflashing’ or ‘cyberstalking’

The review of national laws to ensure their compliance with international and regional child rights standards is not a one-off exercise. It is an ongoing obligation of States to review their legislation to ensure it complies with its international and regional obligations, including with regard to the criminalization of online child sexual exploitation and abuse offences. As new forms of online child sexual exploitation and abuse start to emerge, consideration should be made as to whether the existing definitions under the law are wide enough to capture these forms of abuse and whether or not specific offences should be introduced to address new means of

such violence. At the time of writing, for example, discussions around the risks to children in the metaverse, including virtual reality gaming and other applications, reinforce the need to assess whether children are sufficiently protected from sexual exploitation and abuse in such spaces.²⁷⁴

Example: Ghana



In Ghana, a decision was made to introduce the specific crime of **cyberstalking** of a child in the Cybersecurity Act (No. 1038) 2020.

'Cyberstalking of a child

65. (1) A person shall not use a computer online service, an Internet service, or a local Internet bulletin board service or any other electronic device to compile, transmit, publish, reproduce, buy, sell, receive, exchange, or disseminate the name, telephone number, electronic mail address, residence address, picture, physical description, characteristics, or any other identifying information on a child in furtherance of an effort to arrange a meeting with the child for the purpose of engaging in sexual intercourse, sexually explicit conduct, or unlawful sexual activity.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than five years and not more than fifteen years.

(3) For the purpose of this Section, "unlawful sexual activity" means a sexual activity characterised by

- (a) a recurrent intense sexual urge of a person,
- (b) a sexually arousing fantasy of a person, or
- (c) the use of an object by a person resulting in the suffering or humiliation of that person, the partner of that person, a child or any other non-consenting partner.'

Example: England and Wales



The draft Online Safety Bill (published on 17 March 2022)²⁷⁵ creates a new offence of sending etc. a photograph or film of genitals, more colloquially referred to as '**cyberflashing**'. However, the provision does not distinguish between adults and children.

This provision was introduced following the recommendation made by the Law Commission (a statutory independent body tasked with conducting research and consultations on legal reform) for a new offence of cyberflashing to be introduced in the law, as it considered that '*this is a problem that is either not addressed well or not addressed at all by the current law*'.²⁷⁶ This recommendation marked a change in the Law Commission's views, as it has previously recommended amending section 66 of the Sexual Offences Act 2003 on exposure to include the sending of images or video recordings of one's genitals. However, following consultation, the Law Commission considered that that approach would be '*too narrow in scope*' as cyberflashing could involve the sending of images or videos of genitals of someone other than the sender.²⁷⁷

'156 Sending etc photograph or film of genitals

In the Sexual Offences Act 2003, after Section 66 insert—

"66A Sending etc photograph or film of genitals

(1) A person (A) who intentionally sends or gives a photograph or film of any person's genitals to another person (B) commits an offence if—

- (a) A intends that B will see the genitals and be caused alarm, distress or humiliation, or
- (b) A sends or gives such a photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether B will be caused alarm, distress or humiliation.

(2) References to sending or giving such a photograph or film to another person include, in particular—

- (a) sending it to another person by any means, electronically or otherwise,
- (b) showing it to another person, and
- (c) placing it for a particular person to find.

(3) “Photograph” includes the negative as well as the positive version.

(4) “Film” means a moving image.

(5) References to a photograph or film also include—

- (a) an image, whether made by computer graphics or in any other way, which appears to be a photograph or film,

(b) a copy of a photograph, film or image within paragraph (a), and

(c) data stored by any means which is capable of conversion into a photograph, film or image within paragraph (a).

(6) A person who commits an offence under this Section is liable—

(a) on summary conviction, to imprisonment for a term not exceeding 12 months or a fine (or both);

(b) on conviction on indictment, to imprisonment for a term not exceeding two years.

(7) In relation to an offence committed before paragraph 24(2) of Schedule 22 to the Sentencing Act 2020 comes into force, the reference in subsection (6)(a) to 12 months is to be read as a reference to six months.”

Consider introducing universal jurisdiction for all offences of child sexual exploitation and abuse, irrespective of whether or not they are facilitated with the use of information and communication technologies, and removing any requirement for ‘double criminality’ for such offences

Online child sexual exploitation and abuse is often transnational in nature and can have a connection to multiple jurisdictions. For example, a child who is resident in State A, but is a national of State B, is filmed being sexually abused in State C, which is live-streamed and viewed by a perpetrator in State D as well as hosted on an online platform headquartered in State E.²⁷⁸ This one example demonstrates the multi-jurisdictional complexities that online child sexual exploitation and abuse cases raise.

To help resolve this issue, national legislation should contain comprehensive jurisdiction clauses providing for extraterritorial jurisdiction to ensure such cases such do not fall through the gaps in national legal frameworks.



The concept of **jurisdiction** has multiple aspects:

- Jurisdiction to regulate may be described as the State's '*power to regulate the actions and activities of certain people by law, policy or administrative act*';
- Jurisdiction to adjudicate may be described as the State's '*power to submit certain persons or entities to its courts*'; and
- Jurisdiction to enforce may be described as the State's '*power to enforce its laws through means of executive or administrative acts, i.e. compel compliance or punish non-compliance*'.²⁷⁹

Under international law, jurisdiction is not necessarily limited to a State's territory, although jurisdiction exercised outside of the territorial boundaries of a State – i.e. '*extraterritorial jurisdiction*' – is normally only exercised if there is a specific permissive rule establishing a link to the asserting State.²⁸⁰ These include:

- The '*active personality principle*' where a link is established based on the nationality of the offender;
- The '*passive personality principle*' where a link is established based on the nationality of the victim;
- The '*protective principle*' where a link is established based on a State's interest to protect its country from a national threat; and
- Universal jurisdiction, which applies to a small number of '*international crimes*' such as genocide, war crimes and crimes against humanity.²⁸¹

'*Universal jurisdiction*' is the concept where a national court is able to prosecute an individual for a crime on the basis that the crime harms the international order.²⁸² Universal jurisdiction is generally invoked when other bases of criminal jurisdiction are not available.²⁸³ For a national court to exercise universal jurisdiction, national legislation recognizing the crime and permitting its prosecution may be generally required.²⁸⁴ Under Article 2.1 of the CRC, States parties are required to respect and ensure the rights set out in the CRC '*to each child within their jurisdiction without discrimination*', which includes respecting and

ensuring the right of the child to protection from all forms of sexual exploitation and abuse contained in Article 34. However, the CRC does not specify the extent to which a State party should establish criminal jurisdiction over child sexual exploitation and abuse offences which do not involve a child within the jurisdiction but elsewhere. Provisions on extraterritorial jurisdiction are instead elaborated in the OPSC and key regional conventions.

OPSC

The OPSC contains obligations for States parties to take '*such measures as may be necessary to establish its jurisdiction*' over OPSC offences that are '**committed in its territory or on board a ship or aircraft registered in that State**' (emphasis added).²⁸⁵ Further, each State party must '*take such measures as may be necessary*' to establish its jurisdiction over OPSC offences '*when the alleged offender is present in its territory and it does not extradite him or her to another State party on the ground that the offence has been committed by one of its nationals*'. States parties also have discretion to establish jurisdiction in the following circumstances:²⁸⁶

- When the alleged offender is a national of that State or a person who has habitual residence in its territory;
- When the victim is a national of that State.

In the OPSC Guidelines, the CRC Committee recommends that States parties extend their criminal jurisdiction further still, to cover cases where the child victim is '*habitually resident in the territory of the State*' and encourages States parties to establish universal jurisdiction for all offences covered by the Optional Protocol regardless of the nationality or habitual residence of the alleged offender or victim.²⁸⁷

In some instances, States require '*double criminality*'. This means that when State A seeks extradition of a person from State B for an offence committed in State A, it must be shown that the offence is not only an offence in State A but also in State B. The CRC Committee has recommended that States remove this requirement for OPSC

offences as this creates a *'gap in the law which enables impunity'*.²⁸⁸

African Charter on the Rights and Welfare of the Child

Regional frameworks provide similar guidance. In General Comment No. 7 on Article 27 of the ACRWC, the ACRWC Committee recommends that legislation *'allow the State to investigate and prosecute all these offences [i.e. offences committed in the State] regardless of whether the alleged perpetrator or the victim is a national of that State'* (emphasis added).²⁸⁹ Further, the ACRWC Committee recommends that, each State party should also establish its jurisdiction over sexual abuse offences that are committed outside its territory when:

- The alleged offender is a national of that State;
- The alleged offender is habitually resident in its territory; or
- The child victim is a national of that State.²⁹⁰

The ACRWC clarifies that it is not necessary for the alleged offender to be present in the territory of the State for action to be taken (for example, an international arrest warrant can be sought where appropriate).²⁹¹ The ACRWC Committee specifically provides the example of an offender in State A watching or ordering the live streaming of a child being sexually abused in State B, the prosecution of which should be established regardless of the nationality or habitual residence of the alleged offender or victim.²⁹²

Like the CRC Committee, the ACRWC Committee encourages States parties to establish universal jurisdiction over offences of online child sexual exploitation and abuse, given the *'increased use of ICT to enable sexual offences against children and the new challenges to territoriality'*.²⁹³ If this is not possible, States parties are encouraged *'to pursue the adoption of multilateral and regional instruments to facilitate prosecutions'*.²⁹⁴

Where multiple jurisdictions make a claim to prosecute an alleged offender of (online) child sexual

exploitation and abuse, the general principles of the CRC should apply, including the best interests of the child being taken as a primary consideration. This is made explicit by the ACRWC Committee which recommends that jurisdictional conflicts *'should be resolved by taking into account the best interests of the child victim or victims, taking into account their identity, needs, family and community situation, and the overall child friendliness of the intended measure or measures'*.²⁹⁵ Legislation should, therefore, ensure the applicability of the general principles of the CRC to cases of online child sexual exploitation and abuse.

Budapest Convention

Under the Budapest Convention, States parties are obliged to establish jurisdiction over the offences outlined in the Convention where the offence is committed in its territory.²⁹⁶ Further, as a general rule, jurisdiction should also be established where the offence is committed in the following circumstances, though States parties may reserve the right not to extend its jurisdiction to offences committed under these circumstances:

- On board a ship flying the State party's flag;
- On board an aircraft registered under the laws of the State party; or
- By one of its nationals if the offence is punishable under the criminal law of the State where it was committed (principle of double criminality) or if the offence is committed outside the territorial jurisdiction of any State.²⁹⁷

The right to not extend jurisdiction in the above circumstances has been criticized as leaving a *'potential loophole'* for *'travelling sex offenders'* as it makes circumstances *'dependent on double criminality'*.²⁹⁸ This provision also does not provide extraterritorial jurisdiction over offences based on the nationality of the victim (which can be contrasted with Article 4 of the OPSC).²⁹⁹ Further, in the event that more than one State party claims jurisdiction, Article 22.5 of the Budapest Convention requires the States to *'where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution'*, rather than making the

decision with the best interests of the child as a primary consideration.

Lanzarote Convention

Article 25 of the Lanzarote Convention requires States parties to take the necessary legislative and other measures to establish jurisdiction over the offences outlined in the Lanzarote Convention when the offence is committed:

- On its territory;
- On board a ship flying the flag of that State party;
- On board an aircraft registered under the laws of that State party;
- By one of its nationals; or
- By a person who has his or her habitual residence in its territory (though States parties reserve the right to opt out of or limit the application of this to certain cases or conditions).³⁰⁰

There is a less onerous obligation for States parties to *'endeavour to take the necessary legislative or other measures'* to establish jurisdiction in relation to a Convention offence where the offence is committed against one of its nationals or a person who has habitual residence in its territory.³⁰¹

Article 25.4 requires States parties to ensure that the double criminality principle does not apply to the following offences committed by its nationals: sexual abuse; offences concerning child prostitution; and certain offences concerning child pornography (recruitment of children to participate; causing children to participate; coercing children to participate; or profiting from or otherwise exploiting a child to participate in pornographic performances). Further, States parties are required to ensure that extraterritorial jurisdiction over certain offences committed by its nationals or by a person who has his or her habitual residence in its territory, is not dependent on a report from the victim or a denunciation from the State in which the offence was committed.³⁰²

Similar to the OPSC, the Lanzarote Convention requires States parties to take the necessary

legislative or other measures to establish jurisdiction over the offences established in the Convention where the State party does not extradite an alleged offender present on its territory solely on the basis of his or her nationality.³⁰³

Other Key Instruments

The EU Directive 2011/93 on Combatting Child Sexual Exploitation and Abuse takes a different approach to the above-mentioned treaties. Rather than focusing on the location or status of the perpetrator or victim, it focuses on where the ICT in question was accessed. Article 17(3) requires Member States to ensure that their jurisdiction includes the situations where any one of the following offences is committed by means of ICT *'accessed from their territory, whether or not it is based on their territory'*:

- Offences relating to child pornography (as it is referred to in the Directive);
- Offences relating to the solicitation of a child for sexual purposes (i.e. grooming); and
- *'In so far as it is relevant'*, an offence concerning child sexual abuse or the incitement, aiding and abetting, or attempt to commit an act of child sexual abuse.

The Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN adopts a similar approach to the OPSC and OPSC Guidelines. The minimum legal standards outlined in Annex 3 of this regional instrument include the establishment of extraterritorial jurisdiction, in accordance with each ASEAN Member State's relevant obligations under Article 4 of the OPSC, for all offences of sexual exploitation of children, including those occurring in the online environment.

ICMEC's Model Legislation on Combatting Grooming of Children for Sexual Purposes recommends including provisions permitting extraterritorial jurisdiction regarding the commission of sexual offences against children (without going into further detail) and the removal of *'dual criminality'* provisions.³⁰⁴

✓ The position outlined in the OPSC and recommendations of the CRC Committee in the OPSC Guidelines (i.e. universal jurisdiction and removal of double criminality) should be regarded as the recommended standard, given that these are the key international instruments concerning the combatting of online child sexual exploitation and abuse.



'[U]niversal jurisdiction does not mean universal investigation'.³⁰⁵ It is still

necessary for State authorities to collaborate with counterparts in other States to collect the evidence necessary for prosecution. See **Part 8: Procedures and methods of investigation of online child sexual exploitation and abuse** for more details.

Child sexual exploitation and abuse offences **should** be recognized by law as extraditable offences, regardless of whether or not they are facilitated by the use of information and communication technologies

Extradition **should not** be conditional upon the existence of an extradition treaty with the other concerned State(s)

Law enforcement authorities **should** be required to take suitable measures to submit the case to its competent authorities for the purpose of prosecution in the event that the alleged perpetrator is not extradited on the basis of the alleged perpetrator's nationality



Extradition refers to *'the formal process whereby a State requests from the requested State the return of a person accused or convicted of a crime to stand trial or serve a sentence in the requesting State'*.³⁰⁶ Extradition regimes are usually governed by (i) national law and (ii) bilateral or multilateral treaties.³⁰⁷

When drafting provisions on extradition, States must comply with the provisions on extradition in the OPSC (as interpreted by the OPSC Guidelines), the Budapest Convention and the Lanzarote Convention, if they are parties to these treaties. Even if they are not, States should have regard to the extradition provisions in these instruments. In summary, the provisions on extradition in these instruments provide a framework under which online child sexual exploitation and abuse offences are regarded as extraditable between States parties or which serve as a legal basis for making an extradition request where no extradition treaty exists but is required by the national law of

a requested State. These provisions highlight the importance of ensuring that perpetrators cannot evade justice through legal loopholes of extradition laws of different States.

OPSC

The inclusion of provisions on extradition in multilateral international instruments, such as the OPSC, is extremely important, as it is a burdensome and lengthy process for States to enter into bilateral extradition treaties with all countries in the world.³⁰⁸ The offences listed in Article 3(1) of the OPSC (broadly, the sale of children, child prostitution and child sexual abuse material offences) are deemed to be *'extraditable offences'* under any extradition treaty existing between States parties and *'shall be included'* as such in every extradition treaty subsequently concluded between them, in accordance with the conditions in such treaties.³⁰⁹ The reference to offences in Article 3(1) of the OPSC means that this extradition

provision does not apply to attempts, complicity or participation in these offences, which are set out in Article 3(2) of the OPSC.³¹⁰ However, the CRC Committee encourages States parties to extend the applicability of extradition to attempts or complicity or participation in any OPSC offences.³¹¹

The effect of Article 5.1 of the OPSC is that the OPSC itself can serve as the legal basis for the extradition. In other words where States have ratified the OPSC there is no need for the two States to have an extradition treaty before granting an extradition request for a person suspected of an OPSC offence.³¹²

Where a State party refuses or fails to extradite a person on the basis of the nationality of the offender (i.e. he or she is a national of the State being asked to extradite him or her), Article 5.5 of the OPSC requires the State to which the request was made to *‘take suitable measures to submit the case to its competent authorities for the purpose of prosecution’*.

The non-extension of extradition to *‘mere possession’* and accessing of child sexual abuse material has been observed as a major gap in the OPSC Guidelines, noting that these acts are not in themselves offences under the OPSC, creating a gap in the extradition framework.³¹³ The same issues arise with regard to the live-streaming of child sexual abuse material, *‘as the accessing of material without possession for further purposes is also not covered’* by Article 3(1) of the OPSC.³¹⁴ It has therefore been suggested that the extradition in the OPSC could be interpreted to also cover attempts to commit, or complicity or participation in OPSC offences, as well as the possession or accessing of child sexual abuse material.³¹⁵ The same arguments have been made with regard to the OPSC’s provisions on mutual legal assistance, for more details on which see **Part 8: Procedures and methods of investigation of online child sexual exploitation and abuse**.

Budapest Convention

Procedures relating to extradition are detailed in Article 24 of the Budapest Convention, which may be described as providing a more comprehensive and *‘cyber-specific’* framework on extradition than the OPSC (above) and Lanzarote Convention (further below).³¹⁶

Article 24(1)(a) of the Budapest Convention applies to extradition between States parties for cybercrimes listed in Articles 2 to 11 of the Convention (these include the offences in Article 9 which relate to child pornography – as it is referred to in the Convention – and intentionally aiding or abetting any such offence),³¹⁷ provided that the crimes are punishable under the laws of both parties by deprivation of liberty for a period of at least one year.³¹⁸ Article 24 proceeds to set out the following requirements in relation to these crimes:

- These crimes are deemed to be included as extraditable offences in any extradition treaty between or among the States parties;
- States parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them;
- If a State party that makes extradition conditional on the existence of a treaty, receives a request for extradition from another State party with which it does not have an extradition treaty, the former State may consider the Budapest Convention as the legal basis for extradition with respect to the criminal offence;
- States parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences as extraditable offences between themselves;
- Extradition shall be subject to the conditions provided for by the law of the requested State party or by applicable extradition treaties, including the grounds on which the requested State party may refuse extradition; and
- If extradition for the criminal offence is refused solely on the basis of the nationality of the alleged perpetrator, or because the requested State party deems that it has jurisdiction over the offence, the

requested State party shall submit the case at the request of the requesting party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting State party in due course.

Lanzarote Convention

Under Article 38(3) of the Lanzarote Convention, if a State party, which makes extradition conditional on the existence of a treaty, receives a request for extradition from a State party with which it does not have such a treaty, it may consider the Lanzarote Convention as the legal basis for extradition in

respect of the offences established in accordance with the Convention.

African Charter on the Rights and Welfare of the Child

In its General Comment No. 7 on the interpretation of Article 27 of the ACRWC, the ACRWC Committee provides that, while the formulation of extradition treaties on a bilateral basis between States is encouraged, *'States are also encouraged to adopt legislative measures that would make extradition for the commission of specified child sexual abuse offences possible without the prior existence of a treaty between the respective countries'*.³¹⁹

The statute of limitations in respect of offences of child sexual exploitation and abuse, irrespective of whether or not it is facilitated by the use of information and communication technologies, **should** be removed

The *'statute of limitations'* is the term used to refer to the national law which sets a time period from the commission of an offence after which a suspect cannot be prosecuted. The CRC Committee provides that child victims of offences of sexual exploitation and abuse are particularly unlikely to report the crime or, if they do report, are only likely to do so many years after the offence has occurred.³²⁰ Feelings of fear, shame or guilt are often among the reasons for children not reporting or reporting when they are older.³²¹ For these reasons, the CRC Committee recommends that States parties avoid establishing a statute of limitations in respect of OPSC offences.³²² Where such statutes exist, the CRC Committee urges States parties to *'adjust them to the particular nature of the crime'* and ensure that time begins to run only when the victim reaches the age of 18.³²³

The ACRWC Committee echoes the CRC Committee's guidance, almost word-for-word, except that it makes its remarks in relation to sexual abuse offences more generally.³²⁴ Neither the CRC Committee nor the ACRWC Committee elaborates on how the statute of limitations should be adjusted to the *'particular nature of the crime'*, though it can

be assumed that the more serious the offence, the longer the limitation period should be.

The Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN refers to the latter guidance provided by the CRC Committee, requiring ASEAN States to ensure that their statutes of limitation for initiating proceedings do not start until the victim reaches the age of 18. However, the first recommendation of the CRC Committee should be preferred, particularly in light of the recommendation to be able to initiate proceedings *ex officio*.³²⁵

This standard is also reflected in UNICEF's reimagined agenda on justice for children, which includes as one of its six goals, that every child survivor of sexual violence, abuse or exploitation receives justice, which includes the removal of limitation periods for sexual offences against children.³²⁶

Ensure minimum penalties/sanctions for adult perpetrators and enhanced penalties/sanctions for aggravating factors including young age of the victim

Setting out effective and appropriate criminal sanctions for individual perpetrators of online child sexual exploitation and abuse in legislation is inherent in a State party's obligations under Article 34 of the CRC. The CRC Committee has emphasized the importance of a child's right to access an effective remedy for breaches of their rights in the digital environment, noting that *'the lack of legislation'* in this area is a barrier to a child's access to justice.³²⁷

The obligation to introduce effective and appropriate criminal sanctions is also specifically mentioned in other international and regional treaties that are relevant to (forms of) online child sexual exploitation and abuse. Under ILO Convention 1999 No. 182 on the Worst Forms of Child Labour, States parties are required to take *'immediate and effective measures'* to prohibit and eliminate the worst forms of child labour as *'a matter of urgency'*, including through penal or other appropriate sanctions.³²⁸ The Budapest Convention requires States parties to adopt such legislation and other measures as may be necessary to ensure that the criminal offences under the Convention are punishable by *'effective, proportionate and dissuasive sanctions, which include deprivation of liberty'*.³²⁹

Various human rights frameworks specifically require States parties to take measures to ensure that child sexual exploitation and abuse is punishable by stricter sanctions than other crimes, as well as similar crimes committed against adults, in order to reflect the seriousness of this violence. The OPSC requires States parties to make OPSC offences punishable by appropriate penalties that take into account their *'grave nature'*.³³⁰ The Arab Convention on Combating Information Technology Offences, which criminalizes pornography,³³¹ provides stricter penalties for *'pornography of children and minors'* (Article 12.2), including offences involving the acquisition of such material or material of children and minors which constitutes an outrage of modesty, committed through information technology or a storage medium for such technology (Article 12.3). More generally, States parties also

commit to increasing the punishment for *'traditional crimes'* when committed by means of information technology (Article 21).

ICMEC's Model Legislation on Combatting Grooming of Children for Sexual Purposes recommends:

- Establishing minimum penalties for perpetrators of online grooming; and
- Enhancing penalties for repeat offenders or aggravating factors, such as the age of the victim or the age difference between the offender and the victim.³³²

With regard to child sexual abuse material, ICMEC recommends specifying criminal sanctions and enhanced punishments that distinguish such material from adult pornography.³³³

Ensure that children alleged as, accused or convicted of a crime, including of online child sexual exploitation and abuse offences, are handled within a separate child justice system in accordance with child-friendly justice principles and procedures

It is well-established under international human rights law that children alleged, accused or convicted of a crime must be handled within a separate child justice system in accordance with child-friendly justice principles and procedures. This obligation stems from Article 40(3) of the CRC, which requires States parties to seek to promote the establishment of laws, procedures, authorities and institutions specifically applicable to these children, including the establishment of a minimum age below which children shall be presumed not to have the capacity to infringe the penal law (commonly referred to as the minimum age of criminal responsibility).

Child justice obligations and standards apply equally to children alleged as, accused or convicted of a crime of online child sexual exploitation and abuse. Evidence indicates that children who commit sexual offences have low rates of sex offending recidivism, with offending in general declining with age.³³⁴

✓ Although it is beyond the scope of this Global Guide to provide a detailed overview of international and regional child justice standards, when developing legislation on online child sexual exploitation and abuse offences, States must comply with their international and regional child justice obligations and should apply recommended standards and good practices in this area.³³⁵

Obligations include:

- Introducing, whenever appropriate and desirable, measures into the law for dealing with children who have committed a crime without resorting to judicial proceedings, and provided that human rights and legal safeguards are fully respected (i.e. diversion);³³⁶ and
- Introducing a range of alternative measures to a detention sentence to ensure that children are dealt with in a manner appropriate to their well-being and proportionate both to their circumstances and the offence (alternative measures).³³⁷

For crimes relating to online child sexual exploitation and abuse, diversion or alternative measures may include developmentally appropriate treatments, involving parents and caregivers where possible.³³⁸

✓ Children who commit a criminal act relating to online child sexual exploitation and abuse when under the minimum age of criminal responsibility must not be handled through the criminal justice system but should be referred to the child protection system if the child is in need of care and protection.

Endnotes

- 173 CRC, Art. 34.
- 174 CRC General Comment No. 25 (2021), para. 116.
- 175 OPSC Guidelines, para. 37.
- 176 These terms are used here instead of 'exploitation of children in/ for prostitution' or 'child sexual abuse material', which are the terms recommended in the Luxembourg Guidelines, in order to mirror the terminology in the OPSC.
- 177 OPSC, Article 3.1(a)(i), (b) and (c).
- 178 Ibid., Article 3.2.
- 179 OPSC Guidelines, para. 9(c).
- 180 ACRWC Committee, General Comment (No. 7 of 2021) on Article 27, July 2021 (ACRWC GC 7), para. 90.
- 181 Budapest Convention, Article 9.1.
- 182 Lanzarote Convention, Articles 3.b. and 18 to 24.
- 183 Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography (the EU Directive 2011/93/EU), Articles 3 to 7.
- 184 Group of African, Caribbean and Pacific States and others, Model Policy Guidelines and Legislative Texts, p. 12, <www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cyber-crimes.pdf>, accessed 10 November 2021.
- 185 The general rule in the CRC, Art. 1; ACRWC, Art. 2; ILO Convention No. 182, Art. 2; Palermo Protocol, Art. 3(d); Lanzarote Convention, Art. 3(a); Luxembourg Guidelines, p. 6.
- 186 Luxembourg Guidelines, p. 8.
- 187 Ibid., pp. 27-28.
- 188 Council of Europe Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, para. 74, <<https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>>, accessed 15 March 2022.
- 189 Reflecting the guidance in the Luxembourg Guidelines, pp. 7-8.
- 190 CRC Committee, General Comment No. 20 (2016) on the implementation of the rights of the child during adolescence, CRC/C/GC/20, 6 December 2016 (CRC Committee General Comment No. 20 (2016)), para. 40. For more details on the minimum age of sexual consent, see pages 7 and 8 of the Luxembourg Guidelines.
- 191 Yarrow, Elizabeth, Anderson, Kirsten, Aplan, Kara, and Watson, Katherine, 'Can a restrictive law serve a protective purpose? The impact of age-restrictive laws on young people's access to sexual and reproductive health services', *Reproductive Health Matters*, vol. 22, no. 44, 2014, pp. 148-156, p. 149.
- 192 CRC Committee General Comment No. 20 (2016), para. 40. For more details on the minimum age of sexual consent, please see pages 7 and 8 of the Luxembourg Guidelines.
- 193 CRC Committee, General Comment No. 13 (2011) on the right of the child to freedom from all forms of violence, CRC/C/GC/13, 18 April 2011, FN 9.
- 194 CRC Committee General Comment No. 20 (2016), para. 40.
- 195 OPSC Guidelines, para. 73.
- 196 ACRWC GC 7, para. 50.
- 197 Ibid., paras. 18 and 55.
- 198 EU Directive 2011/93/EU, para. 20.
- 199 The potential harm and stigma that a child faces when coming into conflict with the law is well-documented in international child justice standards: CRC Committee, General Comment No. 24 (2019) on children's rights in the child justice system, CRC/C/GC/24, 18 September 2019 (CRC General Comment No. 24 (2019)), paras. 15 and 70 <<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-24-2019-childrens-rights-child>>, accessed 10 May 2022; UN Standard Minimum Rules for the Administration of Juvenile Justice, General Assembly Resolution 40/33 of 29 November 1985, commentary to Rules 8 and 11.
- 200 ACRWC GC 7, para. 51.
- 201 Ibid., para. 51.
- 202 ECPAT, INTERPOL and UNICEF, *Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse*, October 2021, p. 35.
- 203 ACRWC GC 7, para. 50.
- 204 Smith, Kercher 2011, referenced in Department of Children, Ministry of Gender Children and Social Protection and UNICEF Ghana, A position paper on harmonizing the age of sexual consent and the age marriage in Ghana, Accra, July 2018, p. 15, <www.unicef.org/ghana/media/2766/file/Harmonizing%20the%20Age%20of%20Sexual%20Consent%20and%20Marriage%20in%20Ghana%20.pdf>, accessed 14 January 2022; ACRWC GC 7, para. 50.
- 205 Department of Children, Ministry of Gender Children and Social Protection and UNICEF Ghana, A position paper on harmonizing the age of sexual consent and the age marriage in Ghana, Accra, July 2018, p. 15, <www.unicef.org/ghana/media/2766/file/Harmonizing%20the%20Age%20of%20Sexual%20Consent%20and%20Marriage%20in%20Ghana%20.pdf>, accessed 14 January 2022; ACRWC GC 7, para. 50.
- 206 ACRWC GC 7, para. 50.
- 207 OPSC, Art. 2.
- 208 OPSC Guidelines, para. 60. See also Luxembourg Guidelines, pp. 37-38.
- 209 Luxembourg Guidelines, p. 38.
- 210 OPSC Guidelines, para. 61; ICMEC, *Child Sexual Abuse Material: Model Legislation and Global Review*, 9th Edition, 2018, pp. 8-10.
- 211 OPSC Guidelines, para. 61.
- 212 Ibid., para. 62.
- 213 Luxembourg Guidelines, p. 36.
- 214 Ibid., p. 41.
- 215 Ibid., pp. 36-38.
- 216 See Luxembourg Guidelines, pp. 37-38 for a more detailed explanation.
- 217 OPSC Guidelines, para. 66; ICMEC, *Child Sexual Abuse Material: Model Legislation and Global Review*, 9th Edition, 2018.
- 218 OPSC Guidelines, para. 67.
- 219 Ibid., para. 42.
- 220 Committee of the Parties to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Committee), Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, 6 June 2019, para. b.
- 221 Lanzarote Committee, Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, 6 June 2019, para. c.
- 222 Ibid., para. d.
- 223 OPSC Guidelines, para. 42; ACRWC GC 7, para. 84.
- 224 All-party Parliamentary Group on Social Media (UK) and the UK Safer Internet Centre, *Selfie Generation, What's behind the rise of self-generated indecent images of children online?*, 2021, pp. 10 and 21.
- 225 Ibid.
- 226 CRC General Comment No. 25 (2021), para. 118.
- 227 Ibid.
- 228 OPSC Guidelines, para. 67.
- 229 Ibid.
- 230 Ibid., paras. 42 and 67.
- 231 ACRWC GC 7, para. 84.
- 232 Ibid., para. 85.
- 233 Ibid.
- 234 Lanzarote Committee, Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, 6 June 2019, para. 1.
- 235 Ibid., para. 2.
- 236 Ibid., para. 3.
- 237 Ibid., para. 4.
- 238 Ibid., para. 5.

- 239 The Lanzarote Committee suggests that there may be some exceptional cases in which a child's self-generated sexual images should be regarded as a criminal offence, but even then suggests that alternative measures to prosecution be considered, Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, 6 June 2019, para. 7.a.
- 240 Lanzarote Committee, Implementation Report on the Protection of Children against Sexual Exploitation and Sexual Abuse Facilitated by Information and Communication Technologies – Addressing the Challenges Raised by Child Self-Generated Sexual Images and/or Video, <<https://rm.coe.int/implementation-report-on-the-2nd-monitoring-round-the-protection-of-ch/1680a619c4>>, accessed 27 April 2022.
- 241 Ibid., para. 42.
- 242 Ibid.
- 243 EU Directive 2011/93/EU, Art. 8(2).
- 244 The term 'child pornography' is used here instead of child sexual abuse material as this is the term used in the Directive.
- 245 EU Directive 2011/93/EU, Art. 8(3).
- 246 These provide a national standard for the recording and counting of notifiable offences recorded by police forces in England and Wales.
- 247 Home Office Counting Rules for Recorded Crime, Crime Recording General Rules, with effect from April 2021, accessible via <<https://www.gov.uk/government/publications/counting-rules-for-recorded-crime>>, accessed 28 March 2022.
- 248 College of Policing, Police Action in Response to Youth Produced Sexual Imagery (Sexting): Briefing Note, p. 5, <www.westsussexscop.org.uk/wp-content/uploads/Police-Action-in-Response-to-youth-produced-sexual-imagerySexting.pdf>, accessed 28 March 2022.
- 249 Ibid.
- 250 Ibid.
- 251 Ibid.
- 252 Paul, Sandra, and Maeve Keenan, Sexting: "Outcome 21" – a solution or part of the problem?, 4 May 2018, <www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/sexting-outcome-21-a-solution-or-part-of-the-problem>, accessed 28 March 2022.
- 253 All-Party Parliamentary Group on Social Media and UK Safer Internet Centre, Selfie Generation: What's behind the rise of self-generated indecent images of children online?, 2021, p. 13.
- 254 OPSC Guidelines para. 67.
- 255 Ibid.
- 256 Lanzarote Committee, Implementation Report on the Protection of Children against Sexual Exploitation and Sexual Abuse Facilitated by Information and Communication Technologies – Addressing the Challenges Raised by Child Self-Generated Sexual Images and/or Videos, p. 37, <<https://rm.coe.int/implementation-report-on-the-2nd-monitoring-round-the-protection-of-ch/1680a619c4>>, accessed 27 April 2022.
- 257 ACRWC GC 7, para. 84.
- 258 OPSC Guidelines, para. 70.
- 259 ACRWC GC 7, para. 81.
- 260 ICMEC, Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 1st Edition, 2017, pp. 16-17.
- 261 OPSC Guidelines, para. 69.
- 262 Luxembourg Guidelines, p. 52.
- 263 CRC General Comment No. 25 (2021), para. 81.
- 264 Luxembourg Guidelines, p. 53.
- 265 OPSC Guidelines, para. 68. The Luxembourg Guidelines and ICMEC propose similar descriptions. See pages 50-51 of the Luxembourg Guidelines and page 9 of ICMEC, Child Sexual Abuse Material: Model Legislation and Global Review, 9th Edition, 2018.
- 266 CRC General Comment No. 25 (2021), para. 81; ICMEC, Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 1st Edition, 2017, pp. 11-14; Lanzarote Convention, Art. 23; EU Directive 2011/93/EU, Art. 6; Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN, Annex 3; UNICEF, Latin America and Caribbean Regional Office and ICMEC, Online Child Sexual Abuse and Exploitation, Guidelines for the Adoption of National Legislation in Latin America, 2016.
- 267 ICMEC, Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 1st Edition, 2017, pp. 11-14.
- 268 Luxembourg Guidelines, p. 51.
- 269 Ibid., pp. 50-51.
- 270 ICMEC, Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 1st Edition, 2017, pp. 11-14.
- 271 Penal Code Law 11.179 of Argentina, Article 131, <<https://observatoriolegislativocele.com/en/Criminal-Code-of-the-Argentine-Republic-Law-11179/>> (ES), accessed 24 May 2022.
- 272 OPSC, Article 3.2
- 273 ACRWC GC 7, para. 135.
- 274 Li, C and Lalani, F. How to address digital safety in the metaverse, World Economic Forum, 14 January 2022, <<https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/>>, accessed 13 May 2022.
- 275 This Bill may have changed since the time of writing this Global Guide.
- 276 Law Commission, Modernising Communications Offences: A Final Report, para. 1.38.
- 277 Ibid., para. 1.40.
- 278 This case study is inspired by a fictional case study adopted by Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', International Journal of Children's Rights, vol. 29, no. 3, (2021), p. 731-732.
- 279 Brenner/Koops, 2004; Osula, 2015; Svantesson/Gerry, 2015, referenced in Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', International Journal of Children's Rights, vol. 29, no. 3, (2021), pp. 731-764, p. 735.
- 280 Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', International Journal of Children's Rights, vol. 29, no. 3, (2021), pp. 731-764, p. 735.
- 281 Ibid., pp 731-764, pp. 735-736 and 739.
- 282 International Justice Resource Center, Universal Jurisdiction, <www.ijrcenter.org/cases-before-national-courts/domestic-exercise-of-universal-jurisdiction/>, accessed 27 April 2022.
- 283 Ibid.
- 284 Ibid.
- 285 OPSC, Article 4.1.
- 286 As Article 4.1 of the OPSC provides that, each State party 'may' (as opposed to 'shall') take such measures as may be necessary to establish jurisdiction over OPSC offences in these circumstances.
- 287 OPSC Guidelines, paras. 83 to 87.
- 288 Ibid., para. 84.
- 289 ACRWC GC 7, para. 92.
- 290 Ibid.
- 291 Ibid.
- 292 Ibid.
- 293 Ibid.
- 294 Ibid.
- 295 Ibid.
- 296 Budapest Convention, Article 22.1.
- 297 Ibid.
- 298 Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', International Journal of Children's Rights, vol. 29, no. 3, (2021), pp. 731-764, p. 741.
- 299 Ibid.
- 300 Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Arts. 25.1 and 25.3.
- 301 Ibid., Art. 25.
- 302 Ibid., Art. 25.6.
- 303 Ibid., Art. 25.7.
- 304 ICMEC, Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 1st Edition, 2017, pp. 18-20.
- 305 Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', International Journal of Children's Rights, vol. 29, no. 3, (2021) pp. 731-764, p. 739.
- 306 UNODC, University Module Services, Module 11: International Cooperation to Combat Transnational Organized Crime, Extradition, <www.unodc.org/e4/en/organized-crime/module-11/key-issues/extradition.html>, 9 December 2021.

- 307 Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', *International Journal of Children's Rights*, vol. 29, no. 3, (2021), pp. 731-764, p. 746.
- 308 Ibid.
- 309 OPSC, Article 5.1.
- 310 Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', *International Journal of Children's Rights*, vol. 29, no. 3, (2021), pp. 731-764, p. 748.
- 311 OPSC Guidelines, para. 89.
- 312 Ibid., para. 88(a).
- 313 Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', *International Journal of Children's Rights*, vol. 29, no. 3, (2021), pp. 731-764, p. 748-749.
- 314 Ibid., p. 749.
- 315 Ibid.
- 316 Ibid., p. 747.
- 317 It may also include attempts to produce child pornography for the purpose of its distribution through a computer system and attempts to distribute or transmit child pornography through a computer system, though States reserve the right not to criminalize such attempts (Article 11).
- 318 Note that Article 24(1)(b) elaborates on which minimum penalty should apply in situations where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or extradition treaty.
- 319 ACRWC GC 7, para. 96.
- 320 OPSC Guidelines, para. 95.
- 321 Ibid., para. 95.
- 322 Ibid., para 95.
- 323 Ibid., para 95.
- 324 ACRWC GC 7, para. 136.
- 325 Ex officio is defined here as 'by virtue of being a holder of a particular office or appointment'.
- 326 UNICEF, #Reimagine Justice for Children, p. 6, <www.unicef.org/media/110176/file/Reimagine-Justice-for-Children.pdf>, 29 March 2022.
- 327 CRC General Comment No. 25 (2021), para. 43.
- 328 Worst Forms of Child Labour Convention 1999 (ILO Convention No. 182), Articles 1 and 7.1.
- 329 Budapest Convention, Article 13.1.
- 330 OPSC, Article 3.3.
- 331 As opposed to pornography of adults, though it is noted that other international and regional instruments reviewed for this Guide do not require or recommend the criminalization of pornography involving adults.
- 332 ICMEC, *Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review*, 1st Edition, 2017, pp. 18-20.
- 333 ICMEC, *Child Sexual Abuse Material: Model Legislation and Global Review*, 9th Edition, 2018, p. 8. It is noted that some jurisdictions criminalize adult pornography, hence the rationale for imposing harsher penalties for offences relating to online child sexual exploitation and abuse is to emphasize its seriousness and distinction from adult pornography.
- 334 UNICEF, *Action to End Child Sexual Abuse and Exploitation: A Review of the Evidence*, 2020, p. 16.
- 335 CRC General Comment No. 24 (2019).
- 336 CRC, Article 40(3)(b); UNICEF, #Reimagine Justice for Children, New York, November 2021, p. 6, <www.unicef.org/media/110176/file/Reimagine-Justice-for-Children.pdf>, accessed 27 April 2022.
- 337 CRC, Article 40(4); UNICEF, #Reimagine Justice for Children, New York, November 2021, p. 6, <www.unicef.org/media/110176/file/Reimagine-Justice-for-Children.pdf>, accessed 27 April 2022.
- 338 UNICEF, *Action to End Child Sexual Abuse and Exploitation*, 2020, p. 16.



7. Duties and responsibilities in relation to business

Checklist of minimum and recommended standards

Duties and responsibilities of businesses **should** be approached using a rights-based approach, within the broader framework of the UN Guiding Principles on Business and Human Rights

Legislation to regulate businesses conduct, services and design of digital technologies **should** place children's rights at the core

Consider requiring businesses to adopt age assurance mechanisms, consistent with data protection and safeguarding requirements, to prevent children's access or exposure to pornography and other illegal or age-restricted sexual content

Consider introducing requirements for businesses to establish 'notice and takedown' procedures, including a requirement to block or remove child sexual abuse material notified to it by a trusted flagger recognized by law

Consider introducing provisions into relevant laws to enable businesses to detect proactively child sexual abuse material accessed or stored on their products and services for the purpose of blocking or removing such materials, provided that the law requires such measures to be legal, necessary and proportionate and the least intrusive option available, without impairing the essence of the individual's right to privacy

Consider making it mandatory for businesses to report online child sexual abuse material to law enforcement or other designated reporting body

Ensure the availability of a range of criminal, civil and administrative sanctions for legal persons for offences relating to online child sexual exploitation and abuse and violations of obligations to protect children from such harms

Businesses are a key stakeholder in the digital environment and are integral to protecting children from online child sexual exploitation and abuse. In order to draft legislation on this topic, it is important to have an understanding of the different categories of business stakeholders along what may be referred to as the '*internet value chain*' and the role that they play in the digital environment.³³⁹ Increasingly, however, businesses across sectors are also developing or deploying digital technologies, so the issues raised in this part can also be relevant to businesses not strictly within the '*technology*' or ICT sectors.



Businesses along the internet value chain vary significantly in size. While it is important that administrative requirements imposed on smaller businesses are proportionate to their size, smaller businesses along the internet value chain may nevertheless host or provide access to large amounts of child sexual abuse materials on the internet.³⁴⁰ Legislating in this area therefore requires careful consultation to ensure a consistent '*zero-tolerance*' approach to online child sexual abuse materials for businesses of all sizes while also ensuring that regulatory responsibilities do not become too onerous.³⁴¹

Using guidance developed by the GSMA, businesses in the internet value chain may be categorized into one of five categories of stakeholders, ranging from businesses that own or sell content rights for distribution on the internet at one end, to businesses providing the user interface (devices, systems and software) at the other (see Figure 2: Internet Value Chain).



Figure 2: Internet Value Chain

Content rights refers to ‘the companies that own, and in most cases sell to others, the rights to various types of content for distribution via the Internet’.³⁴² Content rights include ‘premium rights’ which are professionally produced videos, audio, print and gaming content which are distributed via the internet and paid for through, for example, user subscriptions or advertising. Content rights also include ‘made for digital’ content that is produced for distribution via the internet, from amateur user-generated content to content that is professionally produced.³⁴³ Content may include child sexual abuse material, or adult pornographic and sexual content that can be harmful to children (see **Part 6: Criminalization of online child sexual exploitation and abuse** on the harms that children may experience from being exposed to pornographic content).

Online services consist of a diverse range of consumer and business services provided over the internet through browsers or application platforms.³⁴⁴ As the GSMA notes, it covers ‘much of what most consumers probably perceive to be the actual ‘internet’’.³⁴⁵ Online services may be grouped into five categories,³⁴⁶ which are set out below, each of which may be used by perpetrators as a means of engaging in child sexual exploitation and abuse:

1. E-commerce services: these consist of e-retail companies that sell goods and services online and may be used as a means to produce, distribute, sell etc. child sexual abuse materials

or to offer services to facilitate child sexual exploitation and abuse (such as sexual trafficking of children, the sexual exploitation of children in the context of travel and tourism);

2. Entertainment services: these consist of publishing services, gaming (including platform-based video-gaming with an internet connection), video platforms and music services, which may also be used as a means to produce, distribute, sell, stream etc. child sexual abuse material or to facilitate child sexual exploitation or abuse (for example, via user-to-user communication mechanisms on online gaming). These services may also include adult pornography, or sexual content which may not be suitable for children;
3. Search services: these services include online search engines, such as Google, as well as information and reference services such as Google Maps and Wikipedia. The involvement of these services is critical for combating child sexual exploitation and abuse, for example, by preventing websites hosting child sexual abuse material from appearing in search results;
4. Social and community platforms: these include platforms such as Facebook, Twitter, TikTok, Snapchat and LinkedIn and communications services such as WhatsApp, which may be used by perpetrators to produce, distribute, sell etc. child sexual abuse materials or to facilitate

child sexual exploitation and abuse, such as the online solicitation of children; and

5. Cloud and other e-services: these include paid apps and advertising-based web services and apps, which may be used to, for example, advertise child sexual abuse material.

Enabling technology and services covers *‘a wide range of services that often are not immediately visible to Internet users but are essential to the efficient operation of the overall Internet infrastructure and the websites, servers, platforms, and services that use it’*.³⁴⁷ The involvement of enabling technology and services is therefore important in combating online child sexual exploitation and abuse. These technologies and services include:

1. Enabling platforms, which underpin online services to ensure that they run smoothly, such as design and hosting services and payment platforms;
2. Advertising services, which refers to the intermediary companies that *‘act as agents to serve and place’* ads with service providers which have the end-user-relationship;
3. Managed bandwidth and content delivery providers, which refers to the companies that provide wholesale services that connect telecoms operator networks (which, individually, would fall under the *‘connectivity’* part of the internet value chain), with specialist content delivery networks and adaptation services

that may use private infrastructure and private connections to deliver content and traffic to end users.³⁴⁸

Connectivity refers to suppliers of services, such as broadband, 2G, 3G or 4G data services, which connect end users to the internet via mobile or fixed access. Examples of these suppliers include network providers such as Vodafone, Verizon Wireless and China Mobile, as well as companies that connect internet service providers over fixed networks, such as public Wi-Fi.³⁴⁹

User interfaces may be regarded as the *‘most tangible’* part of the internet value chain as it *‘includes the devices, systems, and software’* used by end users to access the internet and services outlined above. Some companies, such as Apple, produce both the devices and the software.³⁵⁰

More broadly, the term **‘internet service provider’** or **‘ISP’** is often used in relation to the digital environment. This term refers to an organization that provides services for accessing and using the internet. ISPs may also provide other services such as email services, domain registration, web hosting, browser services and software packages.³⁵¹ The network of ISPs is multi-layered. Local ISPs, which sell internet access to customers, may pay larger ISPs for their own access.³⁵² Similarly, larger ISPs may pay even larger ISPs for access until the chain reaches *‘Tier 1’* carriers. Tier 1 carriers are able to reach every network access point without having to pay for access and own the infrastructure in their region.³⁵³

7.1 Detail of minimum and recommended standards

Duties and responsibilities of businesses **should** be approached using a rights-based approach, within the broader framework of the UN Guiding Principles on Business and Human Rights

When developing legislation relating to online child sexual exploitation and abuse in the context of business, it is important to situate the approach to legislative reform within the broader process of addressing child rights issues in the context of business operations.

States parties to the CRC have obligations to respect, protect and fulfil children's rights, which continue to apply in relation to business conduct in the digital environment. The obligation to **respect** 'means that States should not directly or indirectly facilitate, aid and abet any infringement of children's rights' including by businesses and must ensure that 'all actors respect children's rights, including in the context of business activities and operations'.³⁵⁴ The obligation to **protect** requires States parties to protect against infringements of rights guaranteed under the CRC and its Optional Protocols by third parties, including businesses.³⁵⁵ The obligation to **fulfil** 'requires States to take positive action to facilitate, promote and provide for the enjoyment of children's rights', including 'stable and predictable legal and regulatory environments which enable business enterprises to respect children's rights'.³⁵⁶

States parties should adopt or continue to follow this rights-based approach to respect, protect and fulfil the child's right to protection from online child sexual exploitation and abuse. This approach includes States parties developing, monitoring, implementing and evaluating 'legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies'.³⁵⁷

States parties are also required to 'protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment'.³⁵⁸ This obligation includes adopting, monitoring and enforcing laws and regulations, not only to prevent violations of the right to protection from violence in the digital environment, but also to investigate and adjudicate on redressing such violations.³⁵⁹

The CRC Committee also provides specific guidance on the role of businesses in protecting children's rights in the digital environment, which includes the right of the child to be protected from sexual exploitation and abuse, as well as the range of other rights in the CRC such as the child's right to privacy, right to access information and freedom of expression.³⁶⁰ The CRC Committee recognizes the 'respect, protect and remedy' framework set out in the UN Guiding Principles on Business and Human Rights.³⁶¹ Businesses are called upon to 'respect children's rights and prevent and remedy abuse of their rights in relation to the digital environment' while States parties have 'the obligation to ensure that businesses meet those responsibilities'.³⁶²

The Children's Rights and Business Principles also provide a framework for understanding and addressing the impact of business on children's rights.³⁶³

Within this context, States parties are called upon to require businesses to (among other things) undertake due diligence and publish their child rights impact assessments, with special consideration given to the digital environment.³⁶⁴

Example: European Union



On 23 February 2022, the European Commission adopted a proposal for a Directive on corporate sustainability and due diligence.³⁶⁵ If adopted, these reforms would impose a corporate sustainability due diligence duty to address negative human rights and environmental impacts. The duty does not relate solely to children's rights or specifically to the protection of children from online child sexual exploitation and abuse. However, it does illustrate how governments are moving to regulate business conduct and take strides towards mandatory due diligence. At time of writing, the proposed Directive would require the companies within scope to:

- Integrate due diligence into policies;
- Identify actual or potential adverse human rights, which include children's rights and rights included in international conventions, and environmental impacts;
- Prevent or mitigate potential impacts;
- Bring to an end or minimize actual impacts;

- Establish and maintain a complaints procedure;
- Monitor the effectiveness of the due diligence policy and measures; and
- Publicly communicate on due diligence.³⁶⁶

Companies captured by the Directive include all large EU limited liability companies, other EU limited liability companies of a certain size operating in defined high impact sectors, and non-EU companies active in the EU reaching a certain turnover generated in the EU.³⁶⁷ The proposal covers the company's own operations, those of their subsidiaries and their direct and indirect established business relationships.³⁶⁸

In its press release, the European Commission acknowledges that, although several EU Member States have already introduced national rules on due diligence and that some companies have taken voluntary measures, *'there is need for a larger scale improvement that is difficult to achieve with voluntary action'*, hence the introduction of the corporate sustainability due diligence duty.³⁶⁹

Legislation to regulate businesses conduct, services and design of digital technologies **should** place children's rights at the core

One of the primary means of protecting children from online sexual exploitation and abuse is by creating a safe, age-appropriate, inclusive and participatory digital environment for children.³⁷⁰ The CRC Committee recognizes that, although businesses may not be directly involved in perpetuating the sexual exploitation and abuse, *'they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services'*.³⁷¹ Mechanisms to promote the inclusion of children in the digital environment can also give rise to risks, for example, by revealing the location of a child to a potential abuser.³⁷²

To protect children from these risks, the CRC Committee recommends that States parties require *'all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services'*.³⁷³ This requirement should extend to all businesses that target children as well as those which have children as end users or which otherwise affect children.³⁷⁴ States parties should also require such businesses to maintain high standards of transparency and accountability.³⁷⁵

In developing regulatory frameworks, industry codes and terms of service, States parties are still required to ensure compliance with the totality of the rights in the CRC. These include Article 3(1) of the CRC, which establishes the principle and right of the child to have their best interests taken as a primary consideration in all actions concerning the child. As such, States parties are required to ensure that the best interests of the child are central to the development of legislation and policies that shape business activities and operations³⁷⁶ and to all actions regarding the provision, regulation, design, management and use of the digital environment.³⁷⁷ This child rights-based approach to regulating business conduct, services and the design of digital technologies, also referred to as '*rights-by-design*',³⁷⁸ places children's rights and ethics at the core of the issue and is rooted in the UN Guiding Principles on Business and Human Rights and the CRC.

Rights-by-design situates the protection of children from online sexual exploitation and abuse within a more holistic framework that factors in the totality of children's rights, not only the right to protection but also the rights to non-discrimination; life, survival and development; to be heard and participate; to privacy and data protection; to leisure and play; and to information (among others).³⁷⁹ As such, rights-by-design captures considerations relating to privacy-by-design³⁸⁰ and safety-by-design (see the Australia case study below), which States parties should require from digital services and products to minimize the risk of harm to children.³⁸¹ This approach is also important for balancing the child's right to protection and other rights, such as the right to privacy, to ensure that resolutions are reached which place children's interests at the forefront (see the standards relating to privacy further below).

Over recent years, there have been notable and ongoing legislative developments in high-income countries (including Australia and the UK) and in the EU to regulate business conduct to establish a safe digital environment, not only for children but for all users.³⁸² Such laws, which address online safety more broadly, require transparent, inclusive and comprehensive consultation to ensure a rights-by-design approach which not only protects the child's

rights to protection, but also the range of other human and children's rights, including the right to privacy and freedom of expression, political opinion etc. A brief overview of these developments is outlined further below, though it should be noted that the bills/legislative proposals in the EU and the UK are still being consulted on at the time of writing and have not yet reached widespread stakeholder consensus.

Note that at the time of writing, UN Member States are negotiating an International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. While the offences covered by the Convention have yet to be determined, a number of Member States have submitted that online child sexual exploitation and abuse should be included.³⁸³ The proposals on the scope of the Convention include preventive measures limiting the risk of the use of ICTs for criminal purposes/cybercrime for businesses, as well as individuals and States parties.³⁸⁴ This Convention may elaborate or introduce additional standards in this area.

Example: Australia



In 2021, Australia passed the Online Safety Act 2021³⁸⁵, updating its regulatory framework to strengthen the accountability of online service providers for online safety and strengthen the role of the eSafety Commissioner as the independent regulator for online safety.³⁸⁶ Since 2018, the eSafety Commissioner has also been progressing its safety-by-design initiative, which is described by the eSafety Commissioner as follows:

*'Safety by Design puts user safety and rights at the centre of the design and development of online products and services. Rather than retrofitting safeguards after an issue has occurred, Safety by Design focuses on the ways technology companies can minimise online threats by anticipating, detecting and eliminating online harms before they occur. This proactive and preventative approach focuses on embedding safety into the culture and leadership of an organisation. It emphasises accountability and aims to foster more positive, civil and rewarding online experiences for everyone. It encourages technology companies to alter their design ethos from 'moving fast and breaking things' or 'profit at all costs' to 'moving thoughtfully', investing in risk mitigation at the front end and embedding user protections from the get-go.'*³⁸⁷

Research and consultation for the safety-by-design initiative began in 2018 and at the time of writing includes a set of principles that position user safety as a fundamental design consideration, interactive assessment tools for enterprise and start up technology companies, resources for investors and financial entities, and engagement with the tertiary education sector to embed safety-by-design into curricula around the world.³⁸⁸

The Online Safety Act 2021 introduces, among other things, the following:

- 'Basic Online Safety Expectations' for online service providers which establish a 'benchmark for online service providers to be proactive' to protect people from abusive conduct and harmful content online;
- The power of eSafety Commissioner to require online service providers to report on how they meet the Basic Online Safety Expectations and issue statements of compliance or non-compliance with those Expectations;
- Civil penalties for online service providers which fail to meet their reporting obligations.
- A requirement for industry to develop new mandatory codes of conduct to regulate illegal content, such as child sexual abuse material, as well as content deemed inappropriate for children (restricted content) such as pornography;
- Power of the eSafety Commissioner to impose mandatory industry standards if online service providers cannot reach an agreement on the codes or if the codes do not contain appropriate safeguards;
- Power to issue removal notices for child sexual exploitation content, as well as link deletion notices and application removal notices.³⁸⁹

Example: United Kingdom of Great Britain and Northern Ireland



The UK Online Safety Bill (dated 17 March 2022)³⁹⁰ proposes significant reforms including:

- Imposing a duty of care on internet providers of user-to-user services and internet providers of search services, including a specific duty *'to protect children's online safety'* where the services are likely to be accessed by children;³⁹¹
- Introducing obligations on providers of internet services on which pornographic content is published or displayed to ensure that children are not normally able to encounter that content.

The proposed reforms include the introduction of obligations on providers of user-to-user services and search services to:

- Assess their user base and the risks of harm to their users, including whether their services are likely to be accessed by children;
- Take steps to mitigate and manage the risks of harm to individuals arising from illegal content and activity, and (for services likely to be accessed by children) illegal content and activity that is harmful to children;
- Put in place systems and processes which allow users and affected persons to report specified types of content and activity to the service provider, including illegal content such as child sexual abuse material and other content that is harmful to children (if likely to be accessed by children);
- Establish a transparent and easy to use complaints procedure for users and affected persons about, among other things, content which they consider to be illegal or if they consider that the provider is not complying with its duties in relation to illegal content,

content reporting or freedom of expression and privacy;

- Have regard to the importance of protecting users' legal rights to freedom of expression and protecting users from a breach of a legal right to privacy when implementing safety policies and procedures; and
- Put in place systems and processes designed to ensure that detected but unreported child sexual exploitation and abuse content is reported to the National Crime Agency (law enforcement body).³⁹²

Internet service providers which make pornographic content available by way of the service (as opposed to enabling users to generate or share such content) will also be required to ensure that children are not *'normally able'* (a term which is not elaborated in the Explanatory Notes to the Bill) to encounter that content.³⁹³

The Bill proposes new powers for Ofcom, the UK communications regulatory authority, to act as the online safety regulator which will oversee and enforce the regulatory regime.

Example: European Union



In the EU, the European Commission has issued a proposal to develop regulations (commonly referred to as the *'Digital Services Act'*) to establish a single market for digital services.³⁹⁴ The proposal aims to strengthen the transparency and accountability of providers of online platforms, such as social media and marketplaces, and protect the safety of EU citizens and their rights in the digital environment, including children's rights.³⁹⁵ Key features of the proposal include introducing obligations on *'very large online platforms'* to assess the systemic risks posed by their operations and use of services (such as the dissemination of child sexual abuse material and the impact of their services on children's rights more generally) and any potential misuses by the recipients of the service, and to take appropriate mitigating measures.

At the time of writing, the European Parliament has adopted a series of amendments to the proposed Digital Services Act, which includes important amendments for the protection of children's rights.³⁹⁶ These include additional wording to the recitals to clarify that children have rights under the CRC and Article 24 of the Charter of Fundamental Rights of the European Union, with specific reference made to the best interests of the child being a primary consideration in all matters affecting them and the guidance of the CRC Committee in General Comment No. 25 on children's rights in the digital environment.³⁹⁷ Once formally approved by the European Council and European Parliament, the Digital Services Act will be directly applicable to EU companies and non-EU companies offering services in the EU.³⁹⁸

Consider requiring businesses to adopt age assurance mechanisms, consistent with data protection and safeguarding requirements, to prevent children's access or exposure to pornography and other illegal or age-restricted sexual content

A child rights-based approach to digital technologies includes the adoption of controls and appropriate enforcement mechanisms to prevent children from accessing or being exposed to pornography and other illegal or age-restricted content in the digital environment (see **Part 6: Criminalization of online child sexual exploitation and abuse** for the potential harms to children from exposure to pornography, particularly at a young age). Age assurance mechanisms in the digital environment (i.e. *'age verification and age estimation solutions'*)³⁹⁹ are one of the tools that can be used to contribute towards this aim. Such mechanisms may include parental control tools, age-differentiated experiences with password-protected content, block/allow lists, purchase/time controls, opt-out functions, filtering and moderating, and age verification systems.⁴⁰⁰

International and regional standards provide clear recommendations for businesses to introduce age assurance mechanisms. In General Comment No.

25 (2021), in the section on special measures and the protection of children from economic, sexual and other forms of exploitation, the CRC Committee recommends that,

*'Robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements.'*⁴⁰¹

The Council of Europe's Guidelines to Respect, Protect and Fulfil Children's Rights in the Digital Environment call upon States to require the use of age verification mechanisms:

'States should require the use of effective systems of age-verification to ensure children are protected from products, services and content in the digital environment which are legally

*restricted with reference to specific ages, using methods that are consistent with the principles of data minimisation.*⁴⁰²



Age assurance mechanisms should not be used in isolation, but as part of a broader, multi-faceted approach to protecting children online.⁴⁰³

The adoption of age assurance controls and the inclusion of a requirement in legislation is a complex issue that requires careful consultation of the factors at play. These include:

- **Evolving capacities of the child:** The CRC Committee recommends that the measures to protect children in the digital environment should respect the fact that the risks and opportunities associated with children’s engagement in the digital environment change depending on the child’s age and stage of development.⁴⁰⁴ Consequently, protective measures should be age appropriate and take into account the evolving capacities of the child.⁴⁰⁵
- **Legitimate and proportionate limitations on the right to privacy:** Safety measures should not exceed what is necessary to verify or estimate a user’s age and should remain proportionate to the legitimate aim of protecting children from accessing and being exposed to pornography and illegal and age-restricted content.
- **Evidence-based:** Age assurance measures should be informed by the best and most up-to-date research available and draw from a range of disciplines⁴⁰⁶ (see **Part 3: Evidence-based legislation** for more detail).

Example: United Kingdom of Great Britain and Northern Ireland



The Online Safety Bill would impose a duty on user-to-user services, which are likely to be accessed by children, to adopt proportionate measures, systems and processes to mitigate children’s online safety, for example, through the use of age assurance mechanisms.

11. Safety duties protecting children

(1) This Section sets out the duties to protect children’s online safety which apply in relation to regulated user-to-user services that are likely to be accessed by children.

(2) A duty, in relation to a service, to take or use proportionate measures to effectively—

(a) mitigate and manage the risks of harm to children in different age groups, as identified in the most recent children’s risk assessment of the service, and

(b) mitigate the impact of harm to children in different age groups presented by content that is harmful to children present on the service.

(3) A duty to operate a service using proportionate systems and processes designed to—

(a) prevent children of any age from encountering, by means of the service, primary priority content that is harmful to children (for example, by using age verification, or another means of age assurance);

(b) protect children in age groups judged to be at risk of harm from other content that is harmful to children (or from a particular kind of such content) from encountering it by means of the service (for example, by using age assurance).

(4) The duties set out in subsections (2) and (3) apply across all areas of a service, including the way it is operated and used as well as content present on the service, and (among other

things) require the provider of a service to take or use measures in the following areas, if it is proportionate to do so—

- (a) regulatory compliance and risk management arrangements,
- (b) design of functionalities, algorithms and other features,
- (c) policies on terms of use,
- (d) policies on user access to the service or to particular content present on the service, including blocking users from accessing the service or particular content,
- (e) content moderation, including taking down content,
- (f) functionalities allowing for control over content that is encountered, especially by children,
- (g) user support measures, and
- (h) staff policies and practices.

(5) A duty to include provisions in the terms of service specifying—

- (a) how children of any age are to be prevented from encountering primary priority content that is harmful to children (with each kind of primary priority content separately covered);
- (b) how children in age groups judged to be at risk of harm from priority content that is harmful to children (or from a particular kind of such content) are to be protected from encountering it, where they are not prevented from doing so (with each kind of priority content separately covered);
- (c) how children in age groups judged to be at risk of harm from non-designated content that is harmful to children (or from a particular kind of such content) are to be protected from

encountering it, where they are not prevented from doing so.

(6) A duty to apply the provisions of the terms of service referred to in subsection (5) consistently in relation to content which the provider reasonably considers is content that is harmful to children or a particular kind of content that is harmful to children.

(7) A duty to include provisions in the terms of service giving information about any proactive technology used by a service for the purpose of compliance with a duty set out in subsection (2) or (3) (including the kind of technology, when it is used, and how it works).

(8) A duty to ensure that the provisions of the terms of service referred to in subsections (5) and (7) are clear and accessible.

(9) In determining what is proportionate for the purposes of this Section, the following factors, in particular, are relevant—

- (a) all the findings of the most recent children’s risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to children), and
- (b) the size and capacity of the provider of a service.

.....!

The Bill would also impose duties on providers of pornographic content to ensure that children are not normally able to encounter that content.

‘67. Scope of duties about regulated provider pornographic content

A provider of an Internet service within subsection (2) must comply with the duties set out in Section 68 in relation to the service.

An Internet service is within this subsection if—

- (a) regulated provider pornographic content is published or displayed on the service,
- (b) the service is not exempt, and
- (c) the service has links with the United Kingdom.

.....

68. Duties about regulated provider pornographic content

(1) This Section sets out the duties which apply in relation to Internet services within Section 67(2).

(2) A duty to ensure that children are not normally able to encounter content that is regulated provider pornographic content in relation to the service (for example, by using age verification).

(3) A duty to make and keep a written record, in an easily understandable form, of—

- (a) the measures taken or in use, and the policies implemented, to comply with the duty set out in subsection (2), and

(b) the way in which the provider, when deciding on and implementing the measures and policies referred to in paragraph (a), has had regard to the importance of protecting United Kingdom users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a regulated service (including, but not limited to, any such provision or rule concerning the processing of personal data).’

Age verification refers to *‘the age assurance measures that provide the highest level of confidence about a user’s age’*.⁴⁰⁷

Through this amendment, the Online Safety Bill, which previously applied solely to sites which host user-generated material, brings all providers that publish or place pornographic content on their services within the scope of the age verification requirement.⁴⁰⁸ Providers captured by the legal duty include any company that runs such a pornography site accessible to people in the UK.⁴⁰⁹

Consider introducing requirements for businesses to establish ‘notice and takedown’ procedures, including a requirement to block or remove child sexual abuse material notified to it by a trusted flagger recognized by law

‘Notice and takedown’ refers *‘to a company’s procedures for receiving reports that may come from customers, employees, law enforcement or hotlines that child sexual abuse material has been discovered on the company’s networks or services, and for preventing further access and distribution’*.⁴¹⁰ The rationale for notice and takedown procedures is that child sexual abuse material can circulate indefinitely online, perpetuating the harm and trauma to child victims as well as contributing *‘to a perception of the child as a sexual object and risks strengthening the belief among persons with a sexual interest in children that it is “normal”’*.⁴¹¹ It is therefore essential that mechanisms are put

in place to enable users, including children and members of the public, to report child sexual abuse material and to have that material removed or blocked promptly.⁴¹²

The recommendation for businesses to establish notice and takedown procedures at their own initiative is well-established and forms part of several industry guidelines and model frameworks for protecting children online.⁴¹³ Behind the scenes, the process of notice and takedown is often complex with many considerations at play. These include:

- Establishing confidential, free and accessible reporting mechanisms for child victims, service users as well as the public more generally;
- Establishing a process for determining whether or not the material is, in fact, child sexual abuse material and hence illegal and ensuring a consistent approach to the classification of materials as *'illegal'* in cross-border contexts involving jurisdictions with different laws;
- Ensuring the welfare of staff handling the reports and material as well as protecting them from potential prosecution for child sexual abuse material offences for their legitimate handling of the matter;
- Ensuring that the staff handling the reports and accessing materials are vetted and safeguards are in place to ensure materials cannot be circulated and used for other purposes;
- Training staff to ensure that reports are handled in a child-sensitive manner, particularly where reports are received from child victims themselves, and providing links to child protection authorities and support services where appropriate;
- Communicating the *'takedown'* to the relevant ISPs along the internet value chain, which may be located in different jurisdictions; and
- Coordinating with law enforcement bodies to ensure that criminal investigations and victim rescue operations are not compromised and that potential criminal evidence is handled correctly so that it is not rendered inadmissible in any potential proceedings.



Addressing these considerations requires the involvement of multiple stakeholders, including businesses, law enforcement, internet *'hotlines'* or reporting portals, child protection and victim support services, among others, and effective and speedy cross-border communication channels. The ways in which these issues are handled also depend on the national and regional laws applicable to business, victims, perpetrators and other parties involved.

Given these complexities, there is no uniform process for notice and takedowns.⁴¹⁴ However, when developing legislation relating to notice and takedown, it is useful to have a broader understanding of the international framework typically used for these processes and the important role played by internet hotlines and reporting portals:⁴¹⁵

1. State A establishes a reporting portal or internet hotline to which members of the public, including victims, can report the child sexual abuse material.



An internet **'hotline'** refers to a *'dedicated online reporting mechanism to report Internet material suspected to be illegal, including child sexual abuse material'*.⁴¹⁶ A hotline enables the public to anonymously report online material they suspect may be illegal.⁴¹⁷ The establishment of a dedicated hotline is recommended in WeProtect's Model National Response (see Capability 12). Examples of hotlines include:

- CyberTipline operated by the National Center for Missing and Exploited Children (NCMEC) which is the national centralized reporting system in the USA;⁴¹⁸
- Internet Watch Foundation hotline in the UK;⁴¹⁹
- Online Content Complaints Mechanism operated by the eSafety Commissioner in Australia;⁴²⁰
- APLE hotline in Cambodia;⁴²¹
- Te Protejo hotline in Colombia;⁴²² and
- ECPATPh Internet Hotline in the Philippines.⁴²³

A **'reporting portal'** is a customized webpage where people can report suspected child sexual abuse material.⁴²⁴ Reporting portals provide a mechanism for reporting online child sexual abuse material for countries that do not currently have this facility or the infrastructure to establish a hotline.⁴²⁵ A portal may be established with the support of international organizations, such as the Internet Watch Foundation (IWF). IWF has supported the establishment of approximately 50 reporting portals worldwide.⁴²⁶ Examples of IWF-supported portals include:

- IWF-Zimbabwe reporting portal;⁴²⁷
- IWF-Belize reporting portal;⁴²⁸
- IWF-Pakistan reporting portal.⁴²⁹

2. In the case of reports through an IWF portal, hotline analyst based in the UK will then investigate the report received through the portal or hotline and, if confirmed to be illegal according to UK law, will act to have the content removed from the internet as soon as possible.⁴³⁰
3. Analysts for the portal or hotline assess the material. If it is believed that there is illegal material on that page, the URL on which the material was found is inserted into INHOPE's 'ICCAM' database. The ICCAM system *'then crawls all information found on that URL and the analyst can classify each picture and/or video separately as baseline (internationally illegal according to INTERPOL's criteria), nationally illegal or not illegal'*.⁴³¹



INHOPE is a partnership of hotlines around the world that operate in all EU Member States, Russia, South Africa, North and South America, Asia, Australia and New Zealand.⁴³² INHOPE supports hotlines and their partner organizations through training, best practices, quality assurance and staff welfare.⁴³³ In order to join the INHOPE Network, hotlines have to meet certain criteria outlined in INHOPE's Code of Practice.⁴³⁴

4. The hotline which analysed the material notifies the company and/or hotline (depending on the laws and regulations of the jurisdiction and

arrangements agreed with the hotline) in State B where the URL is located.⁴³⁵

5. The company and/or hotline in State B then act to block or remove the material.
6. The hotline which analysed the material also makes the baseline and national illegal images and videos available to the International Criminal Police Organization (INTERPOL) through ICCAM.⁴³⁶ INTERPOL downloads this material and transfers it to its International Child Sexual Exploitation Image Database (ICSE Database) for reference by national law enforcement organizations across the world.⁴³⁷ See **Part 8: Procedures and methods of investigation of online child sexual exploitation and abuse** for more details.

International standards

The basis for introducing notice and takedown can be found in the OPSC Guidelines, in which the CRC Committee urges States parties to the OPSC to ensure that ISPs *'control, block and remove'* child sexual abuse material *'as soon as possible as part of their prevention measures'*.⁴³⁸ It also recommends that States parties establish *'fast and effective procedures'* for, among other things, removing harmful material involving children to prevent such material from continuing to be accessed and shared, in collaboration with the *'private sector, in particular Internet service providers and social networks'* as well as law enforcement and reporting hotlines.⁴³⁹

Although the OPSC Guidelines do not explicitly require States parties to set out the notice and takedown procedure in the law, formal recognition of the role of a *'trusted flagger'* such as an internet hotline or reporting portal can facilitate the establishment and functioning of the system and ensure that the organizations and their staff that assess the material are not prosecuted for child sexual abuse material offences by virtue of their role in the notice and takedown system.⁴⁴⁰ Self-regulation also relies on voluntary efforts by businesses, which may lead to inconsistent practices across the industry. Consideration should therefore be made to placing notice and takedown

requirements in legislation with a view to ensuring compliance across the industry.

Regional standards

African Charter on the Rights and Welfare of the Child: In interpreting Article 27 of the ACRWC (on the right to protection from sexual exploitation and abuse), the ACRWC Committee reiterates CRC Committee guidance on the establishment of fast and effective procedures for blocking and removing harmful material involving children, in collaboration with law enforcement, reporting hotlines and the private sector. It also makes a clear recommendation for States parties to *‘establish by law the responsibility of ICT companies to block, remove and report child sexual abuse material hosted on their servers, if needs be in collaboration with website owners’* (as well as of financial institutions to block and refuse financial transactions intended to pay for any such offences).⁴⁴¹

The ACRWC Committee further provides that *‘governments’* should take measures including *‘through codes of conduct, establishment of regulatory authorities, legislation or principles of licensing’* to make it *‘obligatory’* for companies to prevent known child sexual abuse material from being made available to users or accessible on their platforms and services, to take appropriate action under their terms of service to remove such material, and to report instances to appropriate authorities.⁴⁴²

Material which may not be *‘illegal on its face’* but which may be connected to child sexual exploitation and abuse *‘with appropriate context and confirmation’*, should be factored into the regulatory frameworks.⁴⁴³

European Union Laws: At the time of writing (noting that the Digital Services Act has yet to be adopted and the EU Commission’s proposals for new regulations on the detection, removal and reporting of child sexual abuse material has not been published at the time of writing), the EU legal framework places obligations on Member States in relation to the removal of child sexual abuse material from the internet, though it does not explicitly

oblige Member States to introduce this requirement in legislation.⁴⁴⁴ Article 25(1) of EU Directive 2011/93 on Combating Child Sexual Exploitation and Abuse specifically requires Member States to take *‘the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory’* and *‘to endeavour to obtain the removal of such pages hosted outside of their territory’* (emphasis added). Such measures may include requiring businesses to implement notice and takedown procedures in relation to material on their online networks and services, although non-legislative measures are sufficient to transpose the Directive *‘if they allow the outcomes specified in Article 25 to be achieved in practice’*.⁴⁴⁵ EU Directive 2000/31 on *‘certain legal aspects of information society services, in particular electronic commerce, in the Internal Market’*, commonly referred to as the *‘E-Commerce Directive’*, also provides a legal basis for the establishment of notice and takedown procedures. The E-Commerce Directive broadly aims to ensure the free movement of online services between the Member States⁴⁴⁶ and covers online services such as:

- News websites;
- Online services which sell (for example, books, financial services, travel services, etc.) or advertise;
- Online services which provide professional services (for example, lawyers, doctors, estate agents), entertainment services or basic intermediary services (for example, internet access, transmission and hosting of information); and
- Free online services funded by advertising, sponsorship.⁴⁴⁷

Online service providers, which act as a mere conduit, or caching or hosting service providers, are not responsible for the information they transmit or host, provided that they fulfil certain conditions.⁴⁴⁸ These conditions include caching or hosting service providers reacting *‘expeditiously’* to remove or disable access to the information once they have knowledge of it (for example, through a notice and takedown procedure).⁴⁴⁹ However, Article 15 of the E-Commerce Directive prohibits Member States from imposing a general obligation on online service

providers acting as mere conduits, or caching or hosting providers, to monitor the information, which they transmit or store, or to actively seek facts or circumstances indicating illegal activity.

The proposed Digital Services Act would elaborate on the existing framework. At the time of writing, Article 14 requires hosting service providers to establish mechanisms which are *'easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means'* by individuals and entities in order to notify the provider of illegal information present on its services. Hosting service providers are required to process and decide on the notices *'in a timely, diligent, non-discriminatory and non-arbitrary manner'*.⁴⁵⁰ Notices which contain certain information and enable a *'diligent'* hosting service provider to establish the illegality of the information in question without conducting a legal or factual examination, are regarded as the basis of actual knowledge or awareness of the illegal content, triggering the provisions on liability of the provider for failing to remove or disable that content.⁴⁵¹

Other notable provisions in the proposed Digital Services Act include:

- Designation of *'trusted flagger'* status to trusted organizations, such as INHOPE, to submit notices of illegal content to online platforms, which must then treat the notice with priority; and
- Establishing a *'digital services coordinator'* to monitor the Digital Services Act and receive complaints regarding violations and permitting the coordinator to request judicial orders to respond to particularly serious and serious infringements, such as orders to ensure the prompt removal of web pages containing or disseminating *'child pornography'*.⁴⁵²

Consistent with the E-Commerce Directive, the proposed Digital Services Act preserves the prohibition against imposing general monitoring obligations on service providers as *'they could disproportionately limit users' freedom of expression and freedom to receive information, and could burden service providers excessively and thus unduly interfere with their freedom to conduct a business'*.⁴⁵³ However, it retains the

option for providers of intermediary services to undertake *'voluntary own-initiative investigations'* or take measures aimed at detecting, identifying and removing, or disabling of access to, illegal content, provided that they apply appropriate safeguards or measures to ensure and demonstrate that the investigations and measures are accurate, non-discriminatory, proportionate, transparent and do not lead to the over-removal of content.⁴⁵⁴ Further, providers of intermediary services are required to *'make best efforts to ensure that where automated means are used, the technology is sufficiently reliable to limit to the maximum extent possible the rate of errors where information is wrongly considered as illegal content'*.⁴⁵⁵



The EU Commission is expected to publish proposals for new regulations detailing the responsibilities of online service providers to detect, remove and report online child sexual abuse material.⁴⁵⁶ The proposals are expected to take the legal responsibilities of ISPs beyond reactive reporting via notice and takedown to more proactive means of detecting, removing and reporting child sexual abuse material. The proposals are expected to be published in May 2022. See further below for more details on proactive detection of child sexual abuse materials.

Council of Europe: The Council of Europe's Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment recommend that Member States should require that businesses and other relevant stakeholders promptly take all necessary steps to, among other things, remove child sexual abuse material materials and, pending their removal, restrict access to such materials found on servers outside of their jurisdiction.⁴⁵⁷

Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN: Under the Regional Plan of Action, ASEAN States commit to endeavour to establish a national legal requirement for private sector companies to remove (and report) child sexual abuse material from their platforms and services when they become aware of it.⁴⁵⁸

Model laws

The Southern African Development Community's⁴⁵⁹ Model Law on Computer Crime and Cybercrime⁴⁶⁰ contains provisions (Sections 34 to 38) concerning the liability of 'access providers',⁴⁶¹ 'hosting providers',⁴⁶² 'caching providers',⁴⁶³ 'hyperlinks providers'⁴⁶⁴ and 'search engine providers' in relation to information accessed, transmitted or stored by them. Under these provisions, the providers are not liable provided that the conditions listed in the provision apply. These conditions include the hosting provider, caching provider and hyperlink provider 'expeditiously' removing or disabling access to the information as outlined in the relevant provision,⁴⁶⁵ providing a legal basis for such businesses to introduce and implement notice and takedown. However, Section 33 of the Model Law clarifies that there is no general obligation on ISPs to monitor the data, which it transmits or stores, or 'to actively seek facts or circumstances indicating an unlawful activity'.

Example: Ghana



The Cybersecurity Act 2020 established the Cyber Security Authority to regulate cybersecurity activities in the country. Its objectives include, among other things, preventing, managing and responding to 'cybersecurity threats and cybersecurity incidents' and ensuring 'a secured and resilient digital ecosystem'.⁴⁶⁶ This includes the establishment of a notice and takedown procedure, which requires the issuance of a court order before the Authority can take steps to have the content taken down, filtered or blocked.

'Blocking, filtering and taking down of illegal content

87. (1) The Authority may, on the order of a court, authorise a service provider to block, filter or take down illegal content and phone numbers used for a malicious purpose which seeks to undermine the cybersecurity of the country.

(2) The grounds for blocking, filtering and taking down illegal content and phone numbers include

.....

(b) the protection of children;

.....

(d) the prevention or investigation of a disorder or a crime;

(e) the protection of health;

.....

(g) the prevention of the disclosure of information received in confidence;

.....

(i) any other ground that the Authority may determine.

(3) A service provider who fails to comply with an authorisation made pursuant to subsection (1) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

(4) Where a contravention under subsection (1) continues, the service provider concerned is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

(5) Where a contravention under subsection (1) continues after one month, a person commits an offence and is liable on summary conviction to a fine of not less than one thousand penalty units and not more than ten thousand penalty units or to a term of imprisonment of not less than one year and not more than five years, or to both.'

Example: Australia



The regulatory regime in Australia, which was strengthened by the Online Safety Act 2021, empowers the eSafety Commissioner to administer a number of notice and takedown schemes. These schemes may be used by individuals to report abusive content relating to children, including child sexual abuse material, and to have this content taken down from the internet. The systems most relevant to addressing online child sexual exploitation and abuse are: the illegal and restricted online content scheme; the cyberbullying scheme; the image-based abuse scheme.⁴⁶⁷

As the legislative framework is extensive, an overview of the schemes is provided with links to the legislation:

Illegal and restricted online content scheme: the eSafety Commissioner has the power to issue a takedown notice in relation to *'seriously harmful illegal content'* (referred to as Class 1 content in the legislation) such as child sexual abuse material. The scheme also empowers the eSafety Commissioner to issue remedial notices to require *'restricted online content'* (Class 2 material) such as non-violent sexual activity which is unsuitable for a child to see, to be placed behind a restricted access system or to remove the content.⁴⁶⁸ Providers have 24 hours to take down the material.⁴⁶⁹

Cyberbullying scheme: the eSafety Commissioner can order online service providers to remove cyberbullying content targeting an

Australian child within 24 hours (prior to the Online Safety Act 2021, the time period was 48 hours).⁴⁷⁰ Cyberbullying content is anything posted on a social media service, relevant electronic service or designated internet service which is intended to target an Australian child, and which has the effect of seriously humiliating, harassing, intimidating, or threatening the child.⁴⁷¹ The content must have first been reported to the online service provider at least 48 hours before it is reported to the eSafety Commissioner,⁴⁷² the rationale being that this is often the fastest way to have the content removed.⁴⁷³

Image-based abuse scheme: this scheme targets the non-consensual sharing, or threatened sharing, of intimate images of individuals (see **Part 6: Criminalization of online child sexual exploitation and abuse**, particularly the minimum standard on child sexual abuse material).⁴⁷⁴ Under the Online Safety Act 2021, the eSafety Commissioner can request that a service provider remove the intimate image, and can alert services to accounts that are being misused to threaten to post intimate images. Online service providers have 24 hours (cut from 48 hours) to take down the images.⁴⁷⁵ The eSafety Commissioner has a range of compliance and enforcement options when investigating image-based abuse.⁴⁷⁶ An intimate image is one which shows private body parts in circumstances where a person would expect to have privacy; private activity, such as getting undressed, using the toilet, showering or bathing, or sexual activity; or a person who would normally wear clothes of religious or cultural significance in public without them.⁴⁷⁷

Consider introducing provisions into relevant laws to enable businesses to detect proactively child sexual abuse material accessed or stored on their products and services for the purpose of blocking or removing such materials, provided that the law requires such measures to be legal, necessary and proportionate and the least intrusive option available, without impairing the essence of the individual’s right to privacy

Many businesses choose to use new technologies and artificial intelligence to detect proactively child sexual abuse materials on their products and services in order to block and remove the material and report it to law enforcement and other mandatory reporting bodies. Examples (at the time of writing) include Microsoft’s ‘PhotoDNA’ technology which permits comparisons of digital images against a hash (unique digital signature of an image) list of child sexual abuse materials created by NCMEC, in order to identify known child sexual abuse materials, even where the materials have been slightly altered.⁴⁷⁸



Legislating on this topic requires careful consultation to ensure the eradication of child sexual abuse materials and the protection of children, while also respecting human rights, particularly the right to privacy.

The right to privacy is enshrined in a range of international conventions and declarations including Article 17 of the International Covenant on Civil and Political Rights and Article 12 of the Universal Declaration of Human Rights and continues to apply in the digital environment. Children, like all individuals, have the right to privacy, which is also enshrined in Article 16 of the CRC.⁴⁷⁹ As well as being vital to children’s agency and dignity, privacy is essential for children’s safety.⁴⁸⁰

However, the individual’s right to privacy is not absolute and may be limited in certain circumstances. Under international standards, it is well-established that any interference with an individual’s right to privacy, including in the digital environment, must be legal, necessary and proportionate.⁴⁸¹ The interference ‘must also be the least intrusive option available and must not impair the essence of the right to privacy’.⁴⁸²

Similarly, as for all individuals, a child’s right to privacy is not absolute and may be limited in certain circumstances. The CRC Committee affirms that any interference with a child’s right to privacy in the digital environment should ‘be provided by law, intended to serve a legitimate purpose, uphold the principle of data minimisation, 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 [CRC]’.⁴⁸³

Means and methods of proactive detection of child sexual abuse materials must therefore fall within the boundaries of these legitimate exceptions to the right to privacy – namely, they must be legal, necessary and proportionate, the least intrusive option available and not impair the essence of the right to privacy.

Discussions concerning end-to-end encryption and the implications of proactive detection on the rights to privacy may arise during the course of legislative consultations and should be approached with care. As highlighted by the CRC Committee, ‘[w]here encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material’.⁴⁸⁴ As above, such measures ‘must be strictly limited according to the principles of legality, necessity and proportionality’.⁴⁸⁵

✓ These complexities and challenges should be consulted on carefully with expert input to ensure that the resulting legislation strikes the right balance between the rights to privacy and protection and other rights, within the boundaries established through international standards outlined above.

Example: European Union



The experience in the EU demonstrates the challenges of legislating in this area as well as concerted efforts to ensure the detection, removal and reporting of child sexual abuse materials from the internet.

The ePrivacy Directive aims to protect fundamental rights and freedoms, particularly the rights to privacy and confidentiality, with respect to the processing⁴⁸⁶ of personal data⁴⁸⁷ in the electronic communications sector, as well as the protection of the legitimate interests of subscribers who are legal persons.⁴⁸⁸

Following the introduction of the European Electronic Communications Code,⁴⁸⁹ the definition of ‘*electronic communications services*’ (to which the ePrivacy Directive applies) was expanded to include ‘*number-independent interpersonal communications services*’,⁴⁹⁰ thereby expanding the remit of the ePrivacy Directive to capture services such as web-based email services, connected wearable devices and certain other digital communication channels.⁴⁹¹ However, the ePrivacy Directive did not contain a legal basis for companies providing such services to voluntarily process or report content or traffic data for the purpose of detecting child sexual abuse material. Providers of these services therefore found themselves in a situation where they were no longer permitted to continue voluntarily using technologies to detect child sexual abuse material from number-independent interpersonal communications.⁴⁹²

Given this barrier in the law, in July 2021, the EU Parliament passed a temporary derogation from the ePrivacy Directive via regulations – the ‘*ePrivacy Derogation*’ – permitting the use of technologies by number-independent interpersonal communications service providers to process personal and other data in order to combat online child sexual abuse.⁴⁹³ The ePrivacy Derogation serves to restrict the right to protection of the confidentiality of these communications for the sole purpose of detecting online child sexual abuse on number-independent interpersonal

communications services and reporting it to law enforcement authorities or to organizations acting in the public interest against child sexual abuse and removing online child sexual abuse material from those services.⁴⁹⁴

This temporary barrier in the law reportedly led to a six-month period in 2021 where some companies stopped reporting child sexual abuse material for fear of violating privacy laws.⁴⁹⁵

The ePrivacy Derogation expires after a period of three years, on 3 August 2024, or at an earlier date when a long-term legal framework enters into force to address this gap.⁴⁹⁶

The EU Commission is expected to replace the interim regulation with new regulations detailing the responsibilities of online service providers to detect, remove and report online child sexual abuse material.⁴⁹⁷ The regulations, which are expected to be published in 2022, will require online service providers to detect and report online child sexual abuse material and report the material to public authorities, taking their legal obligations beyond reactive action in response to notice and takedown requests to more proactive means of detecting child sexual abuse materials. The proposals are also expected to entail the establishment of a European centre to prevent and counter child sexual abuse.⁴⁹⁸

Consider making it mandatory for businesses to report online child sexual abuse material to law enforcement or other designated reporting body

The investigation and prosecution of offences relating to online child sexual exploitation and abuse relies on effective cooperation between the technology industry and law enforcement. This includes businesses reporting offences relating to child sexual abuse materials to law enforcement or other designated reporting body.

The CRC Committee touches on the issue of reporting in the context of encryption, by recommending that where encryption is considered appropriate, States parties should consider appropriate measures enabling *'the detection and reporting of child sexual exploitation and abuse or child sexual abuse material'* (emphasis added), provided that such measures are strictly limited according to the principles of legality, necessity and proportionality (for more details, see the standard on **detection** further above).

The ACRWC Committee also highlights the gap in holding ISPs accountable with some countries having no specific obligation to report child sexual abuse material to authorities for investigation.⁴⁹⁹ It therefore issues a clear recommendation for States parties to require ICT companies to report (as well as block and remove), by law, child sexual abuse material hosted on their servers in collaboration with website owners if needed and to put measures in place (for example, through legislation or principles of licencing, codes of conduct, the establishment of regulatory authorities etc.) to implement this.⁵⁰⁰

Under the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse, ASEAN States agree to introduce a legal requirement for private sector companies to report child sexual abuse material on their platforms and services when they become aware of it.

Example: United Kingdom of Great Britain and Northern Ireland



The Online Safety Bill will replace the UK's existing voluntary reporting regime with a new requirement for companies to report child sexual exploitation and abuse content detected on their platform to the National Crime Agency (the law enforcement agency mandated to fight and cut serious and organized crime). See Part 4, Chapter 2 of the Online Safety Bill published on 17 March 2022 for provisions on *'Reporting Child Sexual Exploitation and Abuse Content'*.⁵⁰¹

In the EU, at the time of writing, the ePrivacy Derogation (see further above) which permits in scope providers to detect child sexual abuse material on their services, only applies where certain conditions are met. These include a requirement for the service provider to report, without delay, *'every case of a reasoned and verified suspicion of online child sexual abuse'* to *'the competent national law enforcement authorities or to organisations acting in the public interest against child sexual abuse'*.⁵⁰² It is expected that new EU regulations, a draft of which was not published at the time of writing, will replace this interim derogation with a new framework requiring online service providers to report (as well as detect and remove) online child sexual abuse (see the standard above on **detection** for more details about these proposals).

Further, the proposed Digital Services Act (see the standard above on **notice and takedown** for details) would introduce a requirement for online platforms to inform the law enforcement or judicial authorities of the relevant Member State(s) concerned promptly of any suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place, and to provide all relevant information available,⁵⁰³ which may cover child sexual exploitation and abuse cases.

Ensure the availability of a range of criminal, civil and administrative sanctions for legal persons for offences relating to online child sexual exploitation and abuse and violations of obligations to protect children from such harms

It is well-established under international and regional standards that States parties have an obligation, subject to the legal principles of the State party, to provide a range of criminal, civil and administrative sanctions for legal persons (i.e. companies, corporations or other entities which have legal rights and are subject to legal obligations) for offences relating to child sexual exploitation and abuse and breaches of obligations to protect children from such harms.

Under the OPSC, subject to the provisions of its national law, each State party is required to take measures, where appropriate, to establish the liability of legal persons for the offences in the OPSC relating to the sale of children, *'child pornography'* and *'child prostitution'* (as they are referred to in the instrument).⁵⁰⁴ Subject to the legal principles of the State party, such liability may be criminal, civil or administrative.⁵⁰⁵

Under the ACRWC framework, the ACRWC Committee recommends that, where corporations or companies facilitate or participate in the commission of an offence related to child sexual exploitation and abuse, for example, the online or offline distribution of child sexual abuse materials, States parties have an obligation to ensure that *'such legal persons can be held liable, under criminal, civil or administrative law, for having committed, attempted to commit, been complicit in or participated in the relevant offences'*.⁵⁰⁶

Under the Budapest Convention, States parties are also required to adopt legislation and other measures as may be necessary to establish corporate liability for criminal offences.⁵⁰⁷ The liability of the legal person may be criminal, civil or administrative.⁵⁰⁸ The legal persons must be subject to *'effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions'*.⁵⁰⁹

Similarly, the EU Directive 2011/93 on Combatting Child Sexual Exploitation and Abuse includes

provisions requiring Member States to ensure that legal persons may be held liable for child sexual exploitation and abuse offences.⁵¹⁰ Member States are first required to *'take the necessary measures'* to ensure that legal persons may be held liable for any of the offences in the Directive *'committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person'*.⁵¹¹ Member States must take the necessary measures to ensure that a legal person held liable pursuant to this provision is *'punishable by effective, proportionate and dissuasive sanctions'*, including criminal or non-criminal fines as well as other sanctions, such as: exclusion from entitlement to public benefits or aid; temporary or permanent disqualification from the practice of commercial activities; placing under judicial supervision; judicial winding-up; or temporary or permanent closure of establishments which have been used for committing the offence.⁵¹²

Second, Member States are required to *'take the necessary measures'* to ensure that legal persons may be held liable where the lack of supervision or control by a person in a leading position made the commission of any of the offences in the Directive for the benefit of the legal person possible by a person under its authority.⁵¹³ Similarly, Member States must take the necessary measures to ensure that a legal person held liable pursuant to this provision *'is punishable by sanctions or measures which are effective, proportionate and dissuasive'* (Article 13.2).

Example: Australia



The Online Safety Act 2021 sets out a range of penalties and enforcement measures for breaches of the Act,⁵¹⁴ including:

- Formal warning;
- Infringement notice (which is a notice setting out the details of an alleged contravention of the Act and specifies a penalty that can be paid instead of further action being taken);⁵¹⁵
- Enforceable undertaking (this is where the person makes a formal promise to act, or refrain from acting, in a certain way to ensure compliance with the Act and which becomes enforceable by a court once the eSafety Commissioner accepts the undertaking);⁵¹⁶
- Court-ordered injunction (this is a ‘court order restraining a person from engaging in conduct, or requiring them to take certain

steps, in relation to a contravention or proposed contravention of the Act’);⁵¹⁷ and

- Court-ordered civil penalty (which is an order requiring a person who has breached a civil penalty provision in the Act to pay a pecuniary sum).

Breaches include, for example, social media service or hosting service provider failing to comply with a ‘*removal notice*’ requiring it to take all reasonable steps to remove the child sexual abuse material notified by the eSafety Commissioner from its platform.

A detailed overview of the range of compliance and enforcement measures under the Online Safety Act 2021 is summarized in the eSafety Commissioner’s Compliance and Enforcement Policy.⁵¹⁸

Endnotes

339 Based on the internet value chain provided by GSMA in, The Internet Value Chain: A study on the economics of the internet, May 2016, <www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf>, accessed 1 December 2021.

340 See for example the submissions made by Internet Watch Foundation to the Joint Select Committee of the UK Parliament on the Online Safety Bill, in which it reports that it sees large amounts of child sexual abuse material hosted on smaller providers largely in the Netherlands and that often, ‘smaller, lesser-known, services are a huge part of the problem’; Written evidence submitted by the Internet Watch Foundation (OSB0110), 21 September 2021, para. 4.10.

341 Written evidence submitted by the Internet Watch Foundation (OSB0110) to the Joint Select Committee of the UK Parliament on the Online Safety Bill, 21 September 2021, para. 4.10. Principle 14 of the UN Guiding Principles on Business and Human Rights also provides that it is the responsibility of all business enterprises, regardless of their size, sector, operational context, ownership and structure to respect human rights. However, the scale and complexity of the means through which enterprises meet that responsibility may vary according to these factors and with the severity of the enterprise’s adverse human rights impacts; United Nations Human Rights Office of the High Commissioner, Guiding Principles on Business and Human Rights, New York and Geneva, 2011, <www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>, accessed 15 February 2022.

342 GSMA, The Internet Value Chain: A study on the economics of the internet, May 2016, p. 14, <www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf>, accessed 1 December 2021.

343 Ibid., p. 14.

344 Ibid., p. 15.

345 Ibid.

346 Ibid., p. 15-17.

347 Ibid., p. 18.

348 Ibid., pp. 18-19.

349 Ibid., p. 19.

350 Ibid., pp. 21-22.

351 Twin, Alexandra, Internet Service Provider, Investopedia, 12 August 2021, <www.investopedia.com/terms/i/isp.asp>, accessed 14 September 2021.

352 Ibid.

353 Ibid.

354 CRC General Comment No. 16 (2013), para. 26.

355 Ibid., para. 28.

356 Ibid., para. 29.

357 CRC General Comment No. 25 (2021), para. 36.

358 Ibid., para. 37.

359 Ibid.

360 CRC General Comment No. 25 (2021), part I.

361 CRC General Comment No. 16 (2013).

362 CRC General Comment No. 25 (2021), para. 35.

- 363 UNICEF, the Global Compact and Save the Children, Children's Rights and Business Principles, https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2Fhuman_rights%2FCRBP%2FChildrens_Rights_and_Business_Principles.pdf, accessed 13 May 2022.
- 364 CRC General Comment No. 25 (2021), paras. 38-39.
- 365 European Commission, Just and sustainable economy: Commission lays down rules for companies to respect human rights and environment in global value chains, Press release, Brussels, 23 February 2022, <www.ec.europa.eu/commission/presscorner/detail/en/ip_22_1145>, accessed 30 March 2022.
- 366 Ibid.
- 367 Ibid.
- 368 Ibid.
- 369 Ibid.
- 370 International Telecommunication Union, Guidelines for Industry on Child Online Protection, 2020 edition, p. 5, <www.unicef.org/media/90796/file/ITU-COP-guidelines%20for%20industry-2020.pdf>, accessed 22 April 2022.
- 371 CRC General Comment No. 25 (2021), para. 37.
- 372 Ibid., para. 88.
- 373 Ibid., para. 39.
- 374 Ibid.
- 375 Ibid.
- 376 CRC General Comment No. 16 (2013), para. 15.
- 377 CRC General Comment No. 25 (2021).
- 378 Designing for Children's Rights, Key Principles, Version 1.3.1.
- 379 Designing for Children's Rights, Key Principles, Version 1.3.1. See also Pothong, K. and Livingstone, S., UK "Secure by Design" vs Australian "Safety by Design," 29 September 2021, <<https://blogs.lse.ac.uk/parenting4digitalfuture/2021/09/29/secure-by-design/>>, accessed 31 March 2022.
- 380 Privacy-by-design is an approach that requires 'privacy to be incorporated into networked data systems and technologies, by default.' The Information and Privacy Commissioner of Ontario, Canada, has developed seven 'foundational principles' for privacy-by-design. These principles are that: (1) privacy-by-design should be proactive not reactive and preventative not remedial; (2) privacy should be the default setting; (3) privacy should be embedded into the design; (4) privacy-by design should enable full-functionality, i.e. it is a positive-sum, "win-win" game, not a zero-sum game; (5) privacy-by-design should enable end-to-end security and provide full-life-cycle protection; (6) visibility and transparency of business practices and technology; (7) respect for user privacy and user-centric; Favoukian, A., Privacy by Design: The 7 Foundational Principles, Information and Privacy Commissioner, Ontario, Canada, <www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>, accessed 31 March 2022.
- 381 CRC General Comment No. 25 (2021), paras. 70 and 116.
- 382 Pothong, Kruakae, and Livingstone, Sonia, UK "Secure by Design" vs Australian "Safety by Design," 29 September 2021, <<https://blogs.lse.ac.uk/parenting4digitalfuture/2021/09/29/secure-by-design/>>, accessed 31 March 2022.
- 383 United Nations, First Session of the Ad Hoc Committee, <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html>
- 384 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Proposals on objectives and scope of the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, A/AC.291/CRP.8, 24 February 2022, <www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/V2201067.pdf>, accessed 1 April 2022.
- 385 Online Safety Act 2021 (No. 76, 2021), <www.legislation.gov.uk/Details/C2022C00052/Html/Text>, accessed 1 April 2022.
- 386 eSafety Commissioner, Online Safety Act 2021: Fact Sheet, <www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf>, accessed 1 April 2022.
- 387 eSafety Commissioner, Safety by Design, <www.esafety.gov.au/industry/safety-by-design>, accessed 4 April 2022.
- 388 Ibid.
- 389 eSafety Commissioner, Online Safety Act 2021: Fact Sheet, <www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf>, accessed 4 April 2022.
- 390 Online Safety Bill (UK) published 17 March 2022, <<https://bills.parliament.uk/bills/3137/publications>>, accessed 4 April 2022.
- 391 See Sections 11 and 26 of the Online Safety Bill.
- 392 Explanatory Notes to the Online Safety Bill (drafted dated 17 March 2022), Bill 285-EN, p. 9.
- 393 Ibid.
- 394 European Commission, Proposal for a Regulation of the European Parliament and of the Council on A Single Market for Digital Services (Digital Services Act) And Amending Directive 2000/31/EC, 15 December 2020 (Proposed Digital Services Act), <<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN>>, accessed 25 April 2022.
- 395 Proposed Digital Services Act, Explanatory Memorandum.
- 396 Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)), <www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html>, accessed 25 April 2022.
- 397 Ibid., Amendment 3.
- 398 European Commission, Press Release: Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment, Brussels, 23 April 2022, <www.ec.europa.eu/commission/presscorner/detail/en/ip_22_2545>, accessed 25 April 2022.
- 399 5Rights Foundation, But how do they know it is a child? Age Assurance in the Digital World, October 2021, <www.5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf>, accessed 1 April 2022.
- 400 CRC General Comment No. 25 (2021), para. 114; International Telecommunication Union and UNICEF, Guidelines for Industry on Child Online Protection, 2020 edition, pp. 32-33, <<https://www.unicef.org/media/90796/file/ITU-COP-guidelines%20for%20industry-2020.pdf>>, accessed 13 May 2022; 5Rights Foundation, But how do they know it is a child? Age Assurance in the Digital World, October 2021, <www.5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf>, accessed 1 April 2022.
- 401 CRC General Comment No. 25 (2021), para. 114.
- 402 Council of Europe Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, para. 56, <<https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html>>, accessed 14 May 2022.
- 403 INHOPE, Age verification not a one-stop-shop for protecting children online, 16 August 2021, <www.inhope.org/EN/articles/age-verification-not-a-one-stop-shop-for-protecting-children-online?locale=en>, accessed 15 February 2022; See for example, 5Rights Foundation, But how do they know it is a child? Age Assurance in the Digital World, October 2021, which notes that age assurance is not a 'silver bullet' but is a tool to identify that a service is dealing with a child, <www.5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf>, accessed 1 April 2022.
- 404 CRC General Comment No. 25 (2021), para. 19.
- 405 Ibid., paras. 19 and 82.
- 406 Ibid.
- 407 Explanatory Notes to the Online Safety Bill (drafted dated 17 March 2022), Bill 285-EN, para. 381.
- 408 Ibid.
- 409 Ibid.
- 410 GSMA and UNICEF, Notice and Takedown: Company policies and practices to remove online child sexual abuse material, May 2016, p. 5.
- 411 OPSC Guidelines, para. 41.

- 412 GSMA and UNICEF, Notice and Takedown: Company policies and practices to remove online child sexual abuse material, <www.gsma.com/publicpolicy/wp-content/uploads/2016/05/UNICEF_GSMA2016_Guidelines_NoticeAndTakeDown_PoliciesAndPracticesToRemoveOnlineChildSexualAbuseMaterial.pdf>, accessed 26 April 2022.
- 413 See for example, International Telecommunication Union, Guidelines for industry on Child Online Protection 2020, <www.itu-cop-guide-lines.com/files/ugd/24bbaa_967b2ded811f48c6b57c7c5f68e58a02.pdf>, accessed 26 April 2022; WeProtect Model National Response, particularly Capability 18 on 'Innovative Solution Development', p. 32, <www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf>, accessed 26 April 2022; Five Country Ministerial Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, 5 March 2020, <www.weprotect.org/wp-content/uploads/11-Voluntary-principles-detailed.pdf>, accessed 26 April 2022; GSMA and UNICEF, Notice and Takedown: Company policies and practices to remove online child sexual abuse material, <www.gsma.com/publicpolicy/wp-content/uploads/2016/05/UNICEF_GSMA2016_Guidelines_NoticeAndTakeDown_PoliciesAndPracticesToRemoveOnlineChildSexualAbuseMaterial.pdf>, accessed 26 April 2022.
- 414 See in particular, INHOPE, Notice & Takedown, 2020, <www.inhope.org/media/pages/articles/a-deep-dive-into-notice-and-takedown/1494479061-1595837802/inhope-hotline-notice-and-takedown-procedure-deep-dive.pdf>, accessed 26 April 2022; and GSMA and UNICEF, Notice and Takedown: Company policies and practices to remove online child sexual abuse material, <www.gsma.com/publicpolicy/wp-content/uploads/2016/05/UNICEF_GSMA2016_Guidelines_NoticeAndTakeDown_PoliciesAndPracticesToRemoveOnlineChildSexualAbuseMaterial.pdf>, accessed 26 April 2022.
- 415 Note that other approaches are available, for example, Project Arachnid operated by the Canadian Centre for Child Protection in Canada, Project Arachnid, <www.projectarachnid.ca/en/>, accessed 22 April 2022.
- 416 INHOPE, Hotline Development Guide, <www.inhope.org/EN/hotline-guide?locale=en>, accessed 1 April 2022.
- 417 INHOPE, The Facts, <www.inhope.org/EN/the-facts>, accessed 1 April 2022.
- 418 NCMEC, Overview of the CyberTip Line, <www.missingkids.org/gethelpnow/cybertipline>, accessed 1 April 2022.
- 419 IWF, Report online child sexual abuse images and videos, <<https://www.iwf.org.uk/report/>>, accessed 13 May 2022.
- 420 Office of the eSafety Commissioner, Online Content Complaints, <<https://www.esafety.gov.au/report>>, accessed 1 April 2022.
- 421 APLE, <www.internethotlinecambodia.org/en/reporting-portal/>, accessed 1 April 2022.
- 422 Te Protejo, <www.teprotejocolombia.org/en/inicio-en/>, accessed 22 April 2022.
- 423 ECPATPh Internet Hotline, <www.ecpat.org.ph/report/>, accessed 1 April 2022.
- 424 IWF Reporting Portals, <www.iwf.org.uk/about-us/our-international-work/reporting-portals/>, accessed 1 April 2022.
- 425 Ibid.
- 426 Ibid.
- 427 IWF-Zimbabwe reporting portal, <<https://report.iwf.org.uk/zw/>>, accessed 1 April 2022.
- 428 IWF-Belize reporting portal, <<https://report.iwf.org.uk/bz/>>, accessed 1 April 2022.
- 429 IWF-Pakistan reporting portal, <<https://report.iwf.org.uk/pk/>>, accessed 1 April 2022.
- 430 INHOPE, The Facts, <www.inhope.org/EN/the-facts>, accessed 1 April 2022.
- 431 INHOPE, What is ICCAM and Why is it important?, <www.inhope.org/EN/articles/iccam-what-is-it-and-why-is-it-important?locale=en>, accessed 1 April 2022.
- 432 INHOPE, Our Story, <www.inhope.org/EN/our-story>, accessed 1 April 2022.
- 433 Ibid.
- 434 INHOPE, What is a hotline?, <www.inhope.org/EN/articles/what-is-a-hotline>, accessed 1 April 2022.
- 435 For example, in the USA, notices are sent to the corporation, which is then required by law to notify NCMEC, although in practice, hotlines can make simultaneous notifications to the company and NCMEC; Online key stakeholder interview, international organization, 25 March 2022.
- 436 INHOPE, What is ICCAM and Why is it important?, <www.inhope.org/EN/articles/iccam-what-is-it-and-why-is-it-important?locale=en>, accessed 1 April 2022.
- 437 Ibid.
- 438 OPSC Guidelines, para. 41.
- 439 Ibid., para. 103.
- 440 Online individual interview, international organization, 25 March 2022.
- 441 ACRWC GC 7, paras. 137 and 140.
- 442 ACRWC GC 7, para. 141.
- 443 ACRWC GC 7, para. 142.
- 444 European Commission, Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 872 final, Brussels, 16 December 2016, <<https://eur-lex.europa.eu/legal-content/EN/TX/?uri=CELEX%3A52016DC0872>>, accessed 24 May 2022.
- 445 Ibid.
- 446 EU Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), Article 1.1.
- 447 EUR-Lex, E-Commerce Standard EU Rules, <www.eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:32000L0031>, accessed 10 December 2021.
- 448 Ibid.
- 449 See E-Commerce Directive, Article 13.1(e) in relation to caching providers and Article 14(1)(b) in relation to hosting providers.
- 450 Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)), Amendment 211, <www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html>, accessed 25 April 2022.
- 451 Ibid.
- 452 Proposed Digital Services Act, Article 19 and Recital 82, as amended by Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)), Amendment 12, <www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html>, accessed 25 April 2022.
- 453 Ibid., Amendments 25, 56, 302 and 316
- 454 Ibid., Article 6(1).
- 455 Ibid.
- 456 European Commission, Fighting child sexual abuse: detection, removal and reporting of illegal content online: About this Initiative, <www.ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en>, accessed 25 April 2022.
- 457 Council of Europe Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, paras. 61-66.
- 458 Association of Southeast Asian Nations, Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN (2021-2025), October 2021, <https://asean.org/wp-content/uploads/2021/11/4.-ASEAN-RPA-on-COEA_Final.pdf>, accessed 13 May 2022.
- 459 Member States: Angola; Botswana; Comoros; Democratic Republic of Congo; Eswatini; Lesotho; Madagascar; Malawi; Mauritius; Mozambique; Namibia; Seychelles; South Africa; Tanzania; Zambia; and Zimbabwe; Southern African Development Community, Member States, <www.sadc.int/member-states/>, accessed 10 November 2021.

- 460 To view the Model Law, please see the full Southern African Development Community (SADC) Model Law, www.itu.int/en/ITU-D/Cyber-security/Documents/SADC%20Model%20Law%20Cybercrime.pdf, accessed 16 February 2022.
- 461 Defined in the Model Law as ‘any natural or legal person providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network’ (Section 3(2)).
- 462 Defined in the Model Law as ‘any natural or legal person providing an electronic data transmission service by storing of information provided by a user of the service’ (Section 3(13)).
- 463 Defined in the Model Law as ‘any natural or legal person providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information’s onward transmission to other users of the service upon their request’ (Section 3(3)).
- 464 Defined in the Model Law as ‘any natural or legal person providing one or more hyperlinks’ (Section 3(15)); ‘hyperlink’ is defined in the Model Law as ‘characteristic or property of an element such as symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed’ (Section 3(14)).
- 465 See Model Law, Sections 35(a)-(b) for obligations of hosting providers, 36(e) for caching providers and 37 for hyperlink providers.
- 466 Cybersecurity Act 2020 (Ghana), Article 3.
- 467 eSafety Commissioner, Our legislative functions, <www.esafety.gov.au/about-us/who-we-are/our-legislative-functions>, accessed 4 April 2022; eSafety Commissioner, Reporting Form, <www.esafety.gov.au/report/forms>, accessed 4 April 2022.
- 468 eSafety Commissioner, Our legislative functions, <www.esafety.gov.au/about-us/who-we-are/our-legislative-functions>, accessed 4 April 2022; Online Safety Act 2021 (Australia), Part 9, <www.legislation.gov.au/Details/C2022C00052>, accessed 4 April 2022.
- 469 Ibid.
- 470 eSafety Commissioner, Our legislative functions, <www.esafety.gov.au/about-us/who-we-are/our-legislative-functions>, accessed 4 April 2022; Online Safety Act 2021 (Australia), Section 65, <www.legislation.gov.au/Details/C2022C00052>, accessed 4 April 2022.
- 471 Ibid.
- 472 Online Safety Act 2021 (Australia), Section 65, <www.legislation.gov.au/Details/C2022C00052>, accessed 4 April 2022.
- 473 eSafety Commissioner, What you can report to eSafety, <www.esafety.gov.au/report/what-you-can-report-to-esafety>, accessed 4 April 2022.
- 474 Online Safety Act 2021 (Australia), Section 16, <www.legislation.gov.au/Details/C2022C00052>, accessed 4 April 2022.
- 475 Ibid., Sections 77-79 (for time periods) and Part 6 (for the scheme in general)
- 476 eSafety Commissioner, Image-Based Abuse Scheme; Regulatory Guidance, November 2021, <<https://www.esafety.gov.au/sites/default/files/2022-03/Image-Based%20Abuse%20Scheme%20Regulatory%20Guidance.pdf>>, accessed 13 May 2022.
- 477 eSafety Commissioner, Our legislative functions, <www.esafety.gov.au/about-us/who-we-are/our-legislative-functions>, accessed 4 April 2022; Online Safety Act 2021 (Australia), Section 15, <www.legislation.gov.au/Details/C2022C00052>, accessed 4 April 2022.
- 478 Ith, Tracy, Microsoft’s PhotoDNA: Protecting Children and businesses in the cloud, Microsoft, <<https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/>>, accessed 26 April 2022.
- 479 The CRC Committee provides guidance on children’s rights to privacy in the digital environment in its General Comment No. 25 (2021), particularly in Part E (paragraphs 67 to 78).
- 480 CRC General Comment No. 25 (2021), para. 67.
- 481 Toonen v. Australia, CCPR/C/50/D/488/1992, para. 8.3; Van Hulst v. Netherlands, CCPR/C/82/D/903/1999, paras. 7.3 and 7.6; Madhewoo v. Mauritius, CCPR/C/131/D/3163/2018, para. 7.5; Human Rights Committee, Concluding Observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, para. 22, referenced in the Report of the UN High Commissioner for Human Rights on ‘The right to privacy in the digital age’, A/HRC/48/31, 13 September 2021, p 3, <<https://www.ohchr.org/en/calls-for-input/calls-input/2021/right-privacy-digital-age-report-2021>>, accessed 13 May 2022.
- 482 UN High Commissioner for Human Rights, Report on ‘The right to privacy in the digital age’, A/HRC/48/31, 13 September 2021, p 3, <<https://www.ohchr.org/en/calls-for-input/calls-input/2021/right-privacy-digital-age-report-2021>>, accessed 26 April 2022; Human Rights Committee, General Comment No. 31 (2004) on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 26 May 2004, para. 6.
- 483 CRC General Comment No. 25 (2021), para. 69.
- 484 Ibid., para. 70.
- 485 Ibid., para. 70.
- 486 ‘Processing’ of personal data is defined as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’; ePrivacy Directive, Article 2; EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or ‘GDPR’), Articles 4(1) and 94.
- 487 ‘Personal data’ means ‘any information relating to an identified or identifiable natural person (‘data subject’). An ‘identifiable natural person’ is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; ePrivacy Directive, Article 2, which provides that, save as otherwise provided in the ePrivacy Directive, the definitions in EU Directive 95/46/EC and EU Directive 2002/21/EC apply. However, these two latter Directives have been repealed, such that the definitions in the GDPR now apply; GDPR, Articles 4(1) and 94.
- 488 EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), Article 1.1 to 1.2.
- 489 Introduced by EU Directive 2018/1972.
- 490 This is a term used in the European Electronic Communications Code to refer to ‘an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans’; EU Directive 2018/1972, preamble, para. 7.
- 491 Council of the European Union, Press Release: Combating child abuse online – informal deal with European Parliament on temporary rules, 29 April 2021, <www.consilium.europa.eu/en/press/press-releases/2021/04/29/combating-child-abuse-online-informal-deal-with-european-parliament-on-temporary-rules/#/>, accessed 8 November 2021; Hazzard, M. B., A new EEC coming into play: Key points for electronic communications service providers, 15 September 2020, <www.dlapiper.com/en/us/insights/publications/2020/09/new-eecc-coming-into-play-key-points-for-electronic-communications-service-providers/>, accessed 9 November 2021; ePrivacy Derogation, para. 2.

- 492 Mildebrath H, Legislative Train 10.2021, Proposal for a Regulation on a Temporary Derogation From Certain Provisions of the E-Privacy Directive for the Purpose of Combating Child Sexual Abuse Online / AFTER 2020-3, European Parliament, Members' Research Service, 22 October 2021; Council of the European Union, Press Release: Combating child abuse online – informal deal with European Parliament on temporary rules, 29 April 2021, <www.consilium.europa.eu/en/press/press-releases/2021/04/29/combating-child-abuse-online-informal-deal-with-european-parliament-on-temporary-rules/#>, accessed 8 November 2021.
- 493 Privacy Derogation, European Parliament, <www.europarl.europa.eu/doceo/document/A-9-2020-0258AM-039-039_EN.pdf>, accessed 9 November 2021..
- 494 ePrivacy Derogation, para. 23.
- 495 Bateman, Tom, EU plans to fight child sexual abuse online with new law obliging tech firms to report offences, Reuters, <www.euronews.com/next/2022/01/10/eu-plans-to-fight-child-sexual-abuse-online-with-new-law>, accessed 25 April 2022.
- 496 ePrivacy Derogation, para. 23; European Parliament, 'Legislative Train', New Legislation to Fight Child Sexual Abuse Online / After 2021-2, <www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-combating-child-sexual-abuse-online>, accessed 16 February 2022.
- 497 European Commission, Fighting child sexual abuse: detection, removal and reporting of illegal content online: About this Initiative, <www.ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en>, accessed 25 April 2022.
- 498 European Commission, Fighting child sexual abuse: detection, removal and reporting of illegal content online: About this Initiative, <www.ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en>, accessed 25 April 2022; Bateman, Tom, EU plans to fight child sexual abuse online with new law obliging tech firms to report offences, Reuters, <www.euronews.com/next/2022/01/10/eu-plans-to-fight-child-sexual-abuse-online-with-new-law>, accessed 25 April 2022.
- 499 ACRWC GC 7, para. 17.
- 500 Ibid., paras. 137 and 141.
- 501 Online Safety Bill (UK) published 17 March 2022, <https://bills.parliament.uk/bills/3137>, accessed 4 April 2022.
- 502 ePrivacy Derogation, Article 3.1(j).
- 503 Proposed Digital Services Act, Article 21.
- 504 OPSC, Article 3.4.
- 505 Ibid.
- 506 ACRWC GC 7, para. 135.
- 507 Budapest Convention, Article 12.1-12.2.
- 508 Ibid., Article 12.3.
- 509 Ibid., Article 13.2.
- 510 Ibid., Articles 12 and 13.
- 511 Ibid., Article 12.1.
- 512 Ibid., Article 13.1.
- 513 Ibid., Article 12.2.
- 514 Online Safety Act 2021 (particularly sections 162 to 165), <www.legislation.gov.au/Details/C2021A00076>, accessed 27 April 2022.
- 515 eSafety Commissioner, Compliance and Enforcement Policy, December 2021, p. 15, <www.esafety.gov.au/sites/default/files/2022-03/Compliance%20and%20Enforcement%20Policy.pdf>, accessed 27 April 2022.
- 516 Ibid., p. 13.
- 517 Ibid., p. 14.
- 518 Ibid..



8. Procedures and methods of investigation of online child sexual exploitation and abuse

Checklist of minimum and recommended standards

A point of contact **should** be designated in the legislation to receive referrals, leads and tips regarding suspected cases and to provide immediate assistance for the purpose of investigations or proceedings concerning online child sexual exploitation and abuse offences

A national specialized unit **should** be established with an explicit mandate to lead, support and coordinate investigations as well as specialist law enforcement investigation units at subnational level dedicated to investigating online child sexual exploitation and abuse

Consider introducing a legal requirement for staff to have minimum qualifications and complete pre-service and regular in-service training before working on child protection and child sexual exploitation cases, the details of which may be elaborated in secondary legislation or to be determined by the relevant professional regulatory authority or training authority

Legislation **should** establish the powers and procedures for undertaking criminal investigations of online child sexual exploitation and abuse

Undercover investigations **should** be permitted but regulated by law and comply with international human rights standards

Ensure that it is possible to convict an alleged perpetrator of attempting to commit a child sexual exploitation and abuse offence, even where in fact it would have been impossible for the full offence to have been committed (to cover cases where undercover law enforcement pretends to be a child, another offender ('customer') or co-conspirator)

Legislation **should** allow law enforcement to 'triage' cases once reported

Ensure that legislation contains powers for law enforcement to enter a building and seize / remove stored computer data

Ensure that child victims found during search and seizure operations fall within the scope of child protection laws and are referred to the designated child protection authority

Standard operating procedures and inter-agency joint working protocols **should** be put in place to ensure effective coordination between law enforcement, child protection authority and other relevant agencies in safeguarding the child

Consider developing standard operating procedures for the police to assist investigators on the policies and procedures to be followed when undertaking search and seizure to ensure the admissibility of evidence in a court of law

Legislation **should** be adopted to enable their competent authorities to order or obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, particularly where there are grounds to believe that the computer data is particularly vulnerable to loss or modification

Legislation **should** set out provisions relating to the 'chain of custody' of digital data and devices to maintain the integrity of evidence

Consider making formal arrangements to access secure international (and particularly Interpol) image databases and/or developing a national database

States **should** ensure legislation sets out rules on the admissibility of digital and forensic evidence

State law enforcement and criminal investigation and prosecution authorities in the State **should** cooperate and provide mutual legal assistance to equivalent bodies in other States to the widest extent possible for the purposes of investigating and prosecuting online sexual exploitation and abuse of children, including with regard to obtaining evidence, and to identifying and protecting child victims

Ensure that mutual legal assistance with another State is not conditional on the existence of a treaty for mutual legal assistance with that State

8.1 Detail of minimum and recommended standards

The investigation of online child sexual exploitation and abuse requires specialist expertise in both cybercrime and child protection in law enforcement bodies and judicial bodies. It also requires criminal procedure rules which allow for the admissibility and storage of electronic data.

This section looks at investigation by national law enforcement services. Part 8.2 deals with

the investigative structure – namely, the bodies that should investigate online sexual exploitation and abuse of children and the nature of that investigation. Part 8.3 addresses investigative procedures. Part 8.4 deals with international cooperation through mutual legal assistance (MLA). These parts touch on the treatment of victims but support and services for victims is dealt with more specifically in **Part 9**.

8.2 Investigative structure

A point of contact **should** be designated in the legislation to receive referrals, leads and tips regarding suspected cases and to provide immediate assistance for the purpose of investigations or proceedings concerning online child sexual exploitation and abuse offences

Regional standards

The need for a point of contact is contained in the Budapest Convention.⁵¹⁹ Article 35 requires States parties to *'designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer*

systems and data, or for the collection of evidence in electronic form of a criminal offence'.⁵²⁰ Although this is a Council of Europe instrument, it should be noted that the Convention has been ratified by 66 countries, some of which are not members of the Council of Europe.⁵²¹ The WeProtect Global Alliance also recommends that there should be a dedicated law enforcement body with an explicit remit to lead, support and coordinate investigations into child

sexual exploitation and abuse.⁵²² The principal aim of such a unit is to protect the public by receiving child sexual exploitation and abuse referrals from international law enforcement, the public, industry and NGOs as well as from hotlines.

Examples of law enforcement bodies undertaking the ‘point of contact’ role include the Royal Canadian Mounted Police’s National Child Exploitation Crime Centre in Canada, which is the central point of contact for investigations related to the sexual exploitation of children online across the country and internationally when the victim or offender is Canadian. In the UK, it is the National Crime Agency, in Australia it is the Australian Centre to Counter Child Exploitation and in the Philippines it is the Department of Justice Office of Cybercrime.

In most countries, the law enforcement body receiving referrals does not investigate individual cases, though in some countries there may be a brief initial investigation before a case is passed to law enforcement bodies at subnational levels.

✓ All States should establish a national law enforcement unit with an explicit mandate to receive referrals, leads and tips regarding suspected cases.

 Ten national police forces together with EUROPOL and INTERPOL have joined together to form the **Virtual Global Taskforce**.⁵²³ The international alliance is dedicated to the protection of children from online sexual abuse and other transnational child sex offences and shares intelligence assessments with members to target transnational offenders. Its strategic goals include supporting the private sector to improve their protective security by sharing intelligence on the threat to children from online sexual exploitation and abuse. Overall, it aims to make the internet a safer place, identify, locate and help children at risk, and hold perpetrators appropriately to account.



Figure 3: Membership of Virtual Global Task Force. Source: National Crime Agency UK

A national specialized unit **should** be established with an explicit mandate to lead, support and coordinate investigations as well as specialist law enforcement investigation units at sub-national level dedicated to investigating online child sexual exploitation and abuse

There is a need to have trained and skilled specialist law enforcement investigation units at national and subnational level, with responsibility for online child exploitation and abuse. In most countries, the *'point of contact'* body receiving referrals (see above) is not the same as the law enforcement body with responsibility for leading, supporting and coordinating investigations of individual cases, though the two bodies / units may be under the same Ministry. The point of contact body may conduct brief initial investigations to *'triage'* referrals to ensure validity, and in some cases to decide on urgency and prioritization, before passing the case to the national law enforcement unit.

Examples: Republic of the Philippines and the United Kingdom of Great Britain and Northern Ireland

In the **Philippines**, while the Department of Justice Office of Cybercrime is the body designated as the *'point of contact'* for receiving cyber tips, it passes those to the Internet Crimes Against Children Center (PICACC), a multi-agency body comprised of the Philippine National Police Women and Children Protection Center and the National Bureau of Investigations Anti-Human Trafficking Division, working in cooperation with the UK National Crime Agency, the Australian Federal Police, the National Police of the Netherlands and a NGO (the International Justice Mission).

In the **UK**⁵²⁴ once an initial triage is carried out by the National Crime Agency to determine the validity of the report, the case is passed to the Internet Investigations Unit. The Internet Investigations Team will carry out open-source research through for instance, Facebook, Companies House and general Google searches, checks on police systems and intelligence to see if they are known to police and what they are known for. The Internet Investigations Unit will then prepare a *'package'* containing all the

information available on a case and will send the package to the relevant team at local level. The process happens in days.

Regional standards

The Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN commits the ASEAN member States to encourage *'the establishment of a national specialised unit with an explicit remit to lead, support and coordinate investigations'*.⁵²⁵

The role of the online enforcement unit is often wider than just investigating referrals, leads and tips regarding suspected cases.

Examples: New Zealand, Malaysia, United Kingdom of Great Britain and Northern Ireland and Moldova

New Zealand has a specialist police unit known as Online Child Exploitation Across New Zealand (OCEANZ). It:

- Coordinates international investigations into online paedophile networks;
- Identifies child sexual offenders by monitoring social network websites;
- Targets New Zealand child exploitation sites, including those producing images and abuse for financial gain, in an effort to identify and rescue victims;
- Gathers intelligence for sharing with District-based child exploitation squads, the Department of Internal Affairs, Customs and international partners.⁵²⁶

In **Malaysia**, the Sexual Crime and Children Division (D11) within the Royal Malaysian Police

Criminal Investigation Division is responsible for investigating sex crimes against children, including online child sexual exploitation and abuse.⁵²⁷

Moldova has a dedicated Child Protection Unit within the IT Crimes Investigation Department.⁵²⁸ It also has a specialist prosecutor's office: the Prosecutor's Office for Combating Organised Crime and Special Cases dealing with cases related to cybercrime and child sexual exploitation and abuse at national level. In addition, the General Prosecutor's Office has a special Section on Information Technologies and Cyber Crime within the Department of Criminal Investigation and Criminalistics, responsible for general practice in the field, as well as carrying out criminal investigations and representing the State in serious cases relating to child sexual exploitation and abuse.

The designation of the specialist unit may be set out in the law:

Example: Republic of the Philippines



Republic Act No. 10175, An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for other Purposes, 2011

'Section 10:

The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.'

Cases of child sexual abuse and exploitation are often considered as human trafficking cases and also fall under Section 16(g) of Republic Act 9208 as amended by Republic Act 10364 (The Expanded Anti Trafficking Act of 2012).

16(g) The Philippine National Police (PNP) and National Bureau of Investigation (NBI) shall be the

primary law enforcement agencies to undertake surveillance, investigation and arrest of individuals or persons suspected to be engaged in trafficking. They shall closely coordinate with each other and with other law enforcement agencies to secure concerted efforts for effective investigation and apprehension of suspected traffickers. They shall also establish a system to receive complaints and calls to assist trafficked persons and conduct rescue operations.

There are other national law enforcement agencies around the world that have experience in establishing and delivering a dedicated child sexual exploitation and abuse capability, using a multi-stakeholder approach. Requests for advice and support from these agencies can be made through INTERPOL.

✓ Each country should establish regional / local trained and skilled specialist law enforcement investigation units with responsibility for the investigation of online child exploitation and abuse.

Consider introducing a legal requirement for staff to have minimum qualifications and complete pre-service and regular in-service training before working on child protection and child sexual exploitation cases, the details of which may be elaborated in secondary legislation or determined by the relevant professional regulatory authority or training authority

In order to be effective and confident, members of law enforcement bodies dealing with online child sexual exploitation and abuse need contextualized skills training. Ideally, this training should be embedded into formalized pre-service and in-service training programmes. Research indicates that training needs to take place at different levels and that there is also a need for regular refresher training to keep practitioners up to date with the latest technology and new developments.⁵²⁹

Legislation should contain a requirement for staff to have:

- Minimum qualifications necessary to fulfil their roles and responsibilities;

- A minimum amount of training (or mandatory courses) to be completed to work on child protection or child sexual exploitation cases; and
- Protected time for law enforcement personnel to attend such training.

The minimum qualifications and training may be detailed in secondary legislation or as determined by an appropriate training authority or professional regulatory body, so as to provide flexibility to update the requirements as necessary.

For further guidance on training, see **Part 11: Implementation of legislation**.

8.3 Investigative procedures

Legislation **should** establish the powers and procedures for undertaking criminal investigations of online child sexual exploitation and abuse

The starting point is the Budapest Convention which requires each State party to *'adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purposes of specific criminal investigations or proceedings'*.⁵³⁰ This includes the collection of evidence in electronic form of a criminal offence.

Undercover investigations **should** be permitted but regulated by law and comply with international human rights standards

Ensure that it is possible to convict an alleged perpetrator of attempting to commit a child sexual exploitation and abuse offence, even where in fact it would have been impossible for the full offence to have been committed (to cover cases where undercover law enforcement pretends to be a child, another offender ('customer') or co-conspirator).⁵³¹ This means that it is not necessary for there to be an identified child victim and neither does a 'real child' need to be involved in proceedings.

The purpose of undercover (or covert) operations is to prevent child sexual exploitation and to identify victims and perpetrators. Covert operations by law enforcement bodies take a number of different forms:

- For the purposes of intelligence gathering – namely, so that the police know that a crime has occurred and can learn the identity and location of those responsible and, in some countries, whether there are children / victims at the location in need of immediate rescue and care;
- Preventive investigations – for example, through disruption (i.e. ensuring that planned criminal conduct does not happen) or through prevention of further crime by prosecution and conviction; and
- '*Facilitative*' or '*proactive*' methods – deliberate deceptive techniques to create and sustain a false belief, to induce a person to act in accordance with that false belief even if in so doing that person acts against their own best interests: for instance, when a police officer poses as a child to catch people seeking to groom children on the internet.⁵³²

Article 30(5) of the Lanzarote Convention requires State parties to:

'take the necessary legislative or other measures, in conformity with the fundamental principles of its internal law:

- to ensure an effective investigation and prosecution of offences established in accordance with the Convention, allowing, where appropriate, for the possibility of covert operations'

- to enable units or investigative services to identify the victims of offences in particular by analysing child pornography material such as photographs and audiovisual recordings transmitted or made available through the use of information and communication technologies.'

Intercept evidence

'*Intercept*' evidence is the covert interception of private messages in the form of recordings, transcripts or data, of which the user will normally not be aware. The purpose of it is to prevent crime and to identify and interrupt crimes against children which would otherwise go undetected.⁵³³

The extent to which investigative bodies are allowed to use covert interception differs from country to country. However, most countries have laws relating to the obtaining and use of intercept evidence and, as a rule, permit it only in limited circumstances and only with the authorization of the court. Where investigators carry out interception without a lawful order, such evidence will generally not be admissible: i.e., the Court will not allow it to be given in evidence during proceedings. In some jurisdictions, intercept evidence is not used as evidence at all, but rather as '*intelligence*' which allows the investigating body to identify victims and perpetrators of online exploitation and abuse and to obtain further evidence.



Legislation on intercept evidence may distinguish between *'traffic'* data and *'content'* data.

'Traffic' data: This is defined in the Fiji Cybercrime Act of 2021 and the Ghana Cybersecurity Act 2020 as *'any computer data relating to a communication by means of a computer system, generated by a computer system that forms a part in the chain of communication, indicating the origin, destination, route, time, date, size or duration of the communication, or type of underlying service.'*

'Content' data means the content transmitted, distributed or exchanged by means of electronic communications services, such as text, voice, videos, images, and sound; where metadata of other electronic communications services or protocols are transmitted, distributed or exchanged by using the respective services, they are to be considered content data for the respective service.⁵³⁴

'Content data' means the communication content, i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication other than traffic data.⁵³⁵

Example: Fiji



Cybercrime Act 2021

Interception of content data

23.—(1) If on an application made under oath and affidavit, a police officer or other authorised person demonstrates to the satisfaction of a Judge or Magistrate that there are reasonable grounds to authorise the interception of content data and associated traffic data, related to or connected with a person or premises under investigation for one of the following purposes—

- (a) investigation and prosecution of serious offences; or
- (b) to give effect to a mutual assistance request,

a Judge or Magistrate may issue a warrant requiring a service provider to—

- (i) intercept the content data in real-time; and
- (ii) provide that content data to the authorised person as soon as reasonably practicable,

provided that the real-time interception of content data is not to be ordered for a period beyond what is absolutely necessary and, in any event, not exceeding 90 days.

(2) When issuing a warrant under subsection (1), the Judge or Magistrate must be satisfied that—

- (a) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;
- (b) measures are to be taken to ensure that the content data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and content data of any party not part of the investigation; and

(c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(3) When making an application under subsection (1), the police officer or other authorised person must—

(a) provide reasons as to why the content data sought will be available with the person in control of the computer system;

(b) identify and explain with specificity the type of content data suspected will be found on such computer system;

(c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such computer system;

(d) identify and explain with specificity the identified offences in respect of which the warrant is sought;

(e) provide the measures to be taken to prepare and ensure that the content data will be sought and carried out—

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data of any party not part of the investigation.

(4) The period of real-time interception of content data may be extended beyond the 90-day period if, on an application, a Judge or Magistrate authorises an extension for a further specified period of time, not exceeding a further period of 90 days.

Obtaining a warrant can be a lengthy and highly technical process. There is a view in some countries that it should be possible to use intercept evidence in cases involving child sexual exploitation and abuse, even where this has been obtained through interception without a warrant (e.g., recording a conversation without the knowledge of the other party). This is particularly the case where the rules relating to intercept evidence are very strict.

Example: Republic of the Philippines



Expanded Anti-Trafficking in Persons Act 2022

Section 8 – investigation and prosecution of cases

(b) In investigating violations of this Act involving the use of the internet and other digital platforms, LEOS (law enforcement) acting in an undercover capacity who record their communications with a person or persons reasonably believed to have committed, is committing, or is about to commit any of the violations under this Act, shall not be considered as wiretapping or illegal interception, and shall not be liable under the provisions of Republic Act No, 4200 or “the Anti-Wiretapping Law” ...!

Proactive undercover operations

Proactive policing can involve police posing as “customers” or facilitators who sell livestreamed child sexual abuse to order, or posing as children, for instance, on social networking sites, chat rooms, peer-to-peer sites and other settings. In the latter case, the police may take over profiles of children who have already been groomed or create fake profiles and monitor the actions of known sex offenders.⁵³⁶

International and regional guidance

International law does not deal with the extent to which proactive undercover investigations in relation to child sexual exploitation and abuse should be permitted. Despite the lack of international provisions, the CRC Committee in

General Comment No. 25 notes that States parties should take all available preventive, enforcement and remedial measures, including in cooperation with international partners, to facilitate and reduce impediments to investigation of online sexual exploitation and abuse offences.⁵³⁷

The ICMEC publication, *Online Grooming of Children for Sexual Purposes, Model Legislation and Global Review (2017)*, does not have the force of an international or regional convention, but is an important source of good practice. It recommends putting in place provisions permitting covert (undercover) operations to allow for ‘proactive policing’.

At the present time, different countries vary in the degree to which they permit or restrict proactive undercover law enforcement operations. In many jurisdictions undercover officers are not permitted, for instance, to encourage suspects to commit a crime they would not otherwise commit, nor are they permitted to engage in unlawful behaviour themselves in order to obtain evidence or prevent further offending.

✓ States should develop national legislation, if it does not already exist, covering the range of permissible undercover operations or, at the very least, policy guidelines setting out the limits of proactive undercover operations.⁵³⁸

The ICMEC Model Legislation and Global Review also provides that there is a need to ensure legal protection for law enforcement officers involved in covert operations.⁵³⁹ This relates to a controversial issue: the extent to which undercover law enforcement officers should be permitted to engage in unlawful behaviour in order to obtain evidence of online sexual exploitation and abuse, and the consequences of them so doing in terms of the admissibility of such evidence in a prosecution of an alleged perpetrator.

There are a number of justifications for allowing law enforcement to engage in unlawful behaviour in sexual exploitation and abuse cases. For instance, it has been pointed out that before suspected offenders can be prosecuted for sharing online

child sexual abuse materials, the offender must be identified and this sometimes requires infiltration of online networks. This may require police officers to participate in the distribution of child sexual abuse material to maintain cover and covertly identify and catch as many offenders as possible.⁵⁴⁰

Example: Queensland, Australia



In Queensland, Australia, the Police Powers and Responsibilities Act 2000 permits police officers to apply to the courts for permission to commit criminal offences in the course of an investigation.

Section 224: Authorised controlled activity

(1) This section applies if a police officer considers it is reasonably necessary for a police officer to engage in conduct that—

(a) is directed to obtaining evidence of the commission of a controlled activity offence against a person; and

(b) involves the following (a controlled activity)—

.....

(iii) the police officer engaging in conduct for which, apart from section 225, the police officer would be criminally responsible.

Section 225: Protection from liability

(1) This section applies to each of the following persons (a relevant person)—

(a) a person who authorised a controlled activity under section 224;

(b) a person who is or was authorised under this chapter to engage in a controlled activity.

.....

(4) Also, a relevant person does not incur criminal liability for an act done, or omission made—

(a) under an authority given for a controlled activity; and

(b) in accordance with the policy or procedure about controlled activities applying to the particular controlled activity.

(5) In addition, a relevant person does not incur criminal liability for an act done, or omission made, that, because of a controlled activity, was reasonably necessary for protecting the safety of any person.

(6) However, subsection (5) does not relieve a police officer from criminal liability for an act done or omission made if the act or omission results in—

(a) injury to, or the death of, a person; or

(b) serious damage to property; or

(c) a serious loss of property



Taskforce Argos, the focal point for covert intelligence-gathering for online child sexual exploitation in Queensland was established to undertake aggressive pursuit of suspected abusers and those in possession of child sexual abuse materials.⁵⁴¹ Officers from the Taskforce have posed as children to make contact with and gather evidence against offenders. Sometimes the Taskforce, operating on intelligence from other countries, has received information about the administrator of a website distributing and disseminating child sexual abuse material and has taken over control of the site. This has led to identification of many hundreds of users and the rescue of children and has resulted in prosecutions in different countries. In order to uphold the covert nature of their work, however, Taskforce Argos has, in some cases, posted child sexual abuse material itself to prove that it is a *'bona fide'* member of the site and to allow it to keep gaining intelligence on other users. Without the legal framework (see above), police engaging in such conduct would be criminally responsible. Commentators highlight that issues raised by

such operations relate to: whether and to what extent police should be permitted to engage in such conduct; whether a State that does not permit unlawful activity by its own police in controlled circumstances should be permitted to ask the Queensland Taskforce to get involved in investigating sites; and whether evidence gathered from such operations can be used in a prosecution.⁵⁴²

Example: Ecuador



The Organic Integral Criminal Code of Ecuador 2014

Art. 483.- Undercover operations.- Exceptionally, during the course of investigations and under the direction of the Prosecutor's Office, an undercover operation may be planned and executed with the personnel of the Specialized Integral System of Investigation, Legal Medicine and Forensic Sciences, authorizing its agents to infiltrate criminal organizations or groups, concealing their official identity, with the purpose of identifying participants and gathering and compiling information, evidence and convicting elements for the purpose of the investigation.

The undercover agent shall be exempt from criminal or civil liability for crimes whose commission is impossible to avoid, as long as they are a necessary consequence of the development of the investigation and maintain the proper proportionality with it, or else the agent shall be sanctioned in accordance with the legal regulations that apply.

Art. 484.- Guidelines.- The undercover operations shall observe the following guidelines:

1. The undercover operation shall be directed by the specialized unit of the Prosecutor's Office. It may be requested by the specialized staff of the Comprehensive Specialized System of Investigation, Legal Medicine and Forensic Sciences delivering to the Prosecutor the necessary information to justify it.

2. The Prosecutor's authorization must be substantiated and be on a need-to-investigate basis. Time limitations and controls must be implemented to ensure adequate respect for the human rights of persons under investigation or prosecution.

3. The undercover agent shall not be permitted in any case to promote crimes not previously initiated by the investigated parties.

4. The identity given to the undercover agent shall be maintained during the version presented in the proceedings. Authorization to utilize the identity shall not extend for a period exceeding two years, but shall be renewable for two more years with due justification.

5. If required in the investigated case, every undercover agent shall have the same protection as witnesses.

6. The undercover agent's testimony will be valid elements of conviction in the investigation.

7. In cases of carrying out proceedings that require judicial authorization, the Prosecutor shall request authorization from the competent judge by any means, maintaining due discretion.

8. Convicting evidence obtained during unauthorized covert operations shall be devoid of all value.⁵⁴³



All States will need to consider the extent to which, if at all, they will exempt investigators from liability for committing a criminal offence when in the process of drafting new laws or amending laws relating to the investigation of online sexual exploitation and abuse.



Undercover operations are not always carried out by police forces. There are examples of NGOs and online child abuse activist groups that engage in undercover operations from time to time, a practice which can cause evidential problems for the police and prosecutors once the group reports the offence, or the offence is discovered. An *'online child activist group'* or vigilantes refers to members of the public who try to uncover or catch men or women involved in online child exploitation and abuse. It covers a range of actors: from a parent who intercepts a suspicious internet communication and responds as if they were the targeted child, to sophisticated groups conducting targeted operations with an international dimension.⁵⁴⁴ Such activities, even if well intentioned, have the potential to disrupt legitimate covert law enforcement activities, may involve the commission of offences and are not to be recommended.

Legislation **should** allow law enforcement to 'triage' cases once reported

Before looking in detail at the evidential issues that arise with the investigation and prosecution of child sexual exploitation and abuse, it is useful to think about the process: what happens once a case is reported and received by the contact body. Countries receive a huge number of referrals, all of which need to be addressed. One of the challenges is how to ensure that referrals are dealt with speedily and that children are not placed at risk of suffering harm or, for some, further harm.

In a number of countries, and especially in English-speaking countries, the central body receiving referrals conducts a *'triage'* or a determination of urgency. This involves an initial assessment of the referral and some basic intelligence gathering. The intelligence gathering is likely to involve determining to whom the ISP address is registered and the location of that registration; a check on that person's criminal convictions; whether the person is on social media and what information is available about them; whether the person or their family is

known to social services etc. The central body will also attempt to identify the victim. In some cases, it may be a child of the ISP owner though in the majority of cases it will be a child in another location or, potentially, in another country. The ISP owner may, though, have children living in the house. This information will be collated and sent to the relevant police force for the local area in which the person lives.

and abuse is received. Cases are rated in terms of priority, with cases where there is *'first generation'* material (i.e. material that has not been seen before) given particular priority.

If, after triaging, it is decided that action is needed there will be a referral to the local police force with responsibility for investigating child sexual exploitation and abuse offences. This may be a specialized unit or investigations may be undertaken by the general police force.

Figure 4 below shows the steps followed by the Australian Centre to Counter Child Exploitation when a report of online child sexual exploitation

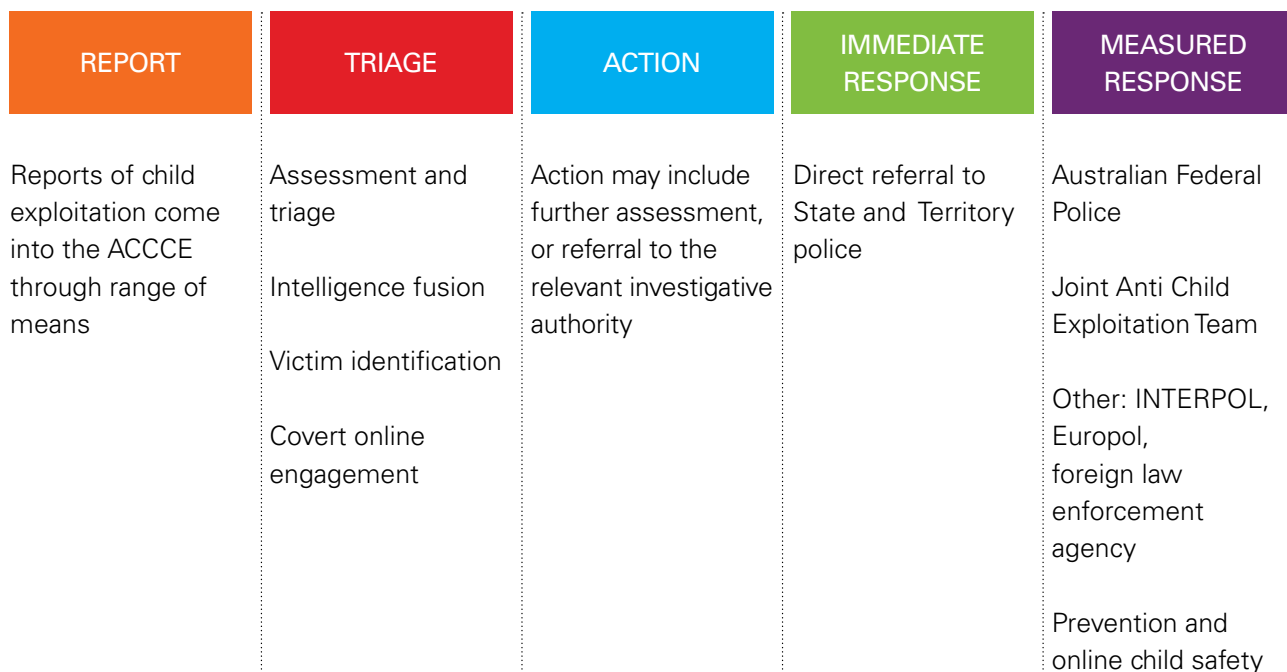


Figure 4: Procedure on receiving a report of online child sexual exploitation and abuse⁵⁴⁵

Ensure that legislation contains powers for law enforcement to enter a building and seize / remove stored computer data

The first step in an investigation at local level will be a visit to the premises of the ISP owner. This is likely to involve the seizure of computers, phones or other electronic materials. In most countries entry into a home and seizure of items will require a warrant and permission to remove items connected to the commission of an offence or to download materials from electronic items where they are not removable on a first visit.

International standards

The OPSC requires that *'State Parties shall take measures for the seizure and confiscation of goods used to commit or facilitate offences under the OPSC and proceeds derived from such offences'*.⁵⁴⁶

Regional standards

The Lanzarote Convention and the Budapest Convention both require States to take legislative measures to empower competent authorities to search and seize computer systems or computer storage mediums.⁵⁴⁷

Article 11 of EU Directive 2011/93 on Combating Child Sexual Exploitation and Abuse provides for seizure and confiscation, requiring that Member States shall take the necessary measures to ensure that their competent authorities are entitled to seize and confiscate instrumentalities and proceeds where offences of sexual exploitation and abuse have been committed.

The Arab Convention on Combating Information Technology Offences also contains procedural provisions that all States parties must commit to adopting in their domestic legal frameworks (Chapter III; Article 22.1). Procedural provisions include the seizure of stored information (Article 27).

Most States have national legislation covering search and seizure in their criminal procedure codes or laws, though these may need to be amended or may require the addition of new provisions relating

to search and seizure of electronic evidence, particularly in relation to child sexual exploitation and abuse offences. As a general rule, it is generally necessary to obtain a warrant from the court before a computer or other devices can be seized.

Example: The Commonwealth Office of Civil and Criminal Justice Reform Model Law on Computer and Computer Related Crime⁵⁴⁸



Article 12.1 Search and seizure warrants

If a magistrate is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data:

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence;

the magistrate [may] [shall] issue a warrant authorising a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data.

Seize is defined as including:⁵⁴⁹

(a) make and retain a copy of computer data, including by using on-site equipment;

(b) render inaccessible, or remove, computer data in the accessed computer system;⁵⁵⁰ and

(c) take a printout of output of computer data.

Examples: Fiji, Egypt and The Republic of the Philippines



Fiji – Cybercrime Act 2021

Search and seizure

16.(1) A police officer or authorised person may apply to a Judge or Magistrate for a warrant to enter a particular location to search and seize a computer, computer program, computer system, computer data storage medium, device or computer data, including to search or obtain similar access to—

(a) a computer system or part thereof and computer data stored therein; and

(b) a computer data storage medium in which computer data may be stored in the territory of the country.

(2) The Judge or Magistrate may issue the warrant, with or without the assistance of an expert, if the Judge or Magistrate is satisfied on the basis of sworn evidence, affidavit, information that there are reasonable grounds to suspect or believe that the computer program, computer system, computer data storage medium, device or computer data in the particular location—

(a) may be material as evidence in proving an offence; or

(b) has been acquired by a person as a result of an offence.

Egypt – Anti-Cyber and Information Law 2018

Temporary Judicial Writs: Article (6)

The investigation body concerned may, as the case may be, issue a substantiated writ to the competent law enforcement officer in respect of one or more of the following matters, for a period not exceeding thirty days renewable for one time, if this will help reveal the truth about the perpetration of an offence punishable under this law:

1. Control, withdrawal, collection, or seizure of data and information or information systems, or tracking them in any place, system, program, electronic support or computer in which they are existing. Its digital evidence shall be delivered to the body issuing the order, provided that it shall not affect the continuity of the system and provision of the service, if so required.

2. Searching, inspecting, accessing and signing in the computer programs, databases and other devices and information systems in implementation of the seizure purpose.

3. The concerned investigation body may order the Service Provider to submit the data or information related to an information system or a technical device under the control of or stored by the Service Provider, as well as the data of the users of its service and the connection traffic made in that system or the technical system.

In all circumstances, the writ issued by the investigation entity must be substantiated. The aforesaid writs shall be appealed before the criminal court concerned, as held in the deliberation room on the dates and according to the procedures stipulated in the criminal procedural law.

Philippines⁵⁵¹ – Republic Act 10175

Section 15. Search, Seizure and Examination of Computer Data. — Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and

(a) To secure a computer system or a computer data storage medium;

(b) To make and retain a copy of those computer data secured;

(c) To maintain the integrity of the relevant stored computer data;

(d) To conduct forensic analysis or examination of the computer data storage medium; and

(e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Ensure that child victims found during search and seizure operations fall within the scope of child protection laws and are referred to the designated child protection authority

Standard operating procedures and inter-agency joint working protocols **should** be put in place to ensure effective coordination between law enforcement, child protection authorities and other relevant agencies in safeguarding the child

Law enforcement officers should remember that there may be children, including victim children on the premises when they enter to search and seize. Joint working protocols should be put in place to ensure that children are referred to the body responsible for child protection, are appropriately

safeguarded and that law enforcement seek to mitigate the impact on children occasioned by the law enforcement intervention (i.e. entry, search, seizure, arrests) through trauma-informed practices, such as the support of a social worker on site.

Consider developing standard operating procedures for the police to assist investigators on the policies and procedures to be followed when undertaking search and seizure to ensure the admissibility of evidence in a court of law

In addition to primary legislation relating to search, seizure, storage and custody of data, States should develop standard operating procedures setting out the actions to be taken by investigators at the crime scene. A standard operating procedure (SOP) is designed to assist investigators by including the policies and the steps that should be taken to ensure that collected evidence is admissible in a court of law, as well as the tools and other resources needed to conduct the investigation.⁵⁵²

Standard operating procedures should cover the identification and collection of digital evidence; the equipment needed to collect digital evidence; securing and evaluating the scene; preliminary interviews; documenting the scene, packaging procedures and records to be kept. It should also detail the steps to be taken when handling digital evidence on mobile devices and internet-enabled objects, such as watches, fitness trackers or home appliances.

Legislation **should** be adopted to enable competent authorities to order or obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, particularly where there are grounds to believe that the computer data is particularly vulnerable to loss or modification

The duties of ISPs to conduct a content analysis and to report online child sexual exploitation and abuse is contained in **Part 7: Duties and responsibilities in relation to business**. This part deals with law enforcement requests to ISPs to access data held by them. Most ISPs have their own provisions relating to the length of time that they preserve data, in order to comply with privacy laws in the jurisdictions in which they work (for example, GDPR). Some may only keep data for days while others may keep it for years. Where ISPs only preserve data for a short period of time, this creates challenges for law enforcement.

Some ISPs may also be bound by privacy legislation, as a result of which States will need to make a request under MLA to access data where this ISP is located in a different State to the State requesting the data. Applying under the MLA can be a time-consuming exercise. Responses from the USA, where many ISPs are based, are taking on average around 10 months to over a year at the time of writing,⁵⁵³ though this may change with the passing of the Clarifying Lawful Overseas Use of Data Act 2018 (the CLOUD Act) and the second Additional Protocol to the Budapest Convention on enhanced co-operation and disclosure of electronic evidence (for which see further below).

Regional standards

Article 16 of the Budapest Convention requires that States shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. Article 16.2 goes on to provide that where a State makes such an order it shall adopt such legislative

and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. Any demand for such data must be subject to the safeguards and conditions contained in its domestic law and regional and international human rights instruments.

Article 18 also permits the competent authority in a State to issue production orders requiring a person in its territory to hand over specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium and an ISP offering its services in the State to submit subscriber information within the service providers possession or control.

Example: The Commonwealth, Office of Civil and Computer Related Crime, Model Law on Computer and Computer Related Crime⁵⁵⁴



Production of data

15. If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that:

- (a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and
- (b) an internet service provider in [enacting country] produce information about persons who subscribe to or otherwise use the service; and
- (c) [a person in the territory of [enacting country] who has access to a specified computer system

process compile specified computer data from the system and give it to a specified person.]

NOTE: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

NOTE: Countries may wish to consider whether subparagraph (c) is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

Disclosure of stored traffic data

Option 1

16. If a police officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the police

officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify:

- (a) the service providers; and
- (b) the path through which the communication was transmitted.

Option 2

16. If a magistrate is satisfied on the basis of an ex parte application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:

- (a) the service providers; and
- (b) the path through which the communication was transmitted.

Legislation **should** set out provisions relating to the 'chain of custody' of digital data and devices to maintain the integrity of evidence

In order for evidence obtained through search and seizure or through legally permitted covert operations to be admissible in court it must be kept securely. States will need to decide where and how such evidence shall be kept. Digital devices (e.g. computers, phones, tablets etc.) potentially holding digital evidence will need to be stored separately from child sexual abuse material obtained from devices. It is of fundamental importance that the integrity of digital evidence is maintained at each phase of the handling of such evidence. The prosecution will need to be able to show, if challenged, that the digital evidence was not altered in any way at the time of search and seizure or while the devices or images are stored awaiting trial. This requires law enforcement to be able to show what is generally referred to as a 'chain of custody'.



The **chain of custody** is 'the process by which investigators preserve the crime (or incident) scene and evidence throughout the life cycle of a case. It includes information about who collected the evidence, where and how the evidence was collected, which individuals took possession of the evidence, and when they took possession of it'.⁵⁵⁵

Example: **Australia**

In Australia, child sexual abuse materials that have been seized and may be used as evidence are kept on a server, separate to the police server, with limited access, making it easier to demonstrate the chain of custody of this digital evidence.

Law enforcers need to be carefully trained and diligent when it comes to the chain of custody of digital evidence.⁵⁵⁶

Legislation or guidelines would benefit from including a range of good practice principles, including:

- When digital evidence is seized, actions should be taken to ensure that the digital evidence cannot be altered in any way. In cases where this is unavoidable, actions should be satisfactorily accounted for.
- When it is necessary for a person to access original digital evidence, that person must be forensically and legally competent to do so.

- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review, if so ordered by the competent authority.
- An individual is responsible for all actions taken with respect to digital evidence while it is in his or her possession.⁵⁵⁷
- Any law enforcement officer who was part of the chain of custody must be made available to provide testimony where this is required by the court. This is critical where there is a quick turnover of staff or movement of an officer to another unit.

Consider making formal arrangements to access secure international (and particularly Interpol) image databases and/or develop a national database

There are a number of countries with access to secure databases holding illegal images and videos of children known to law enforcement. The USA, the UK and Interpol⁵⁵⁸ have all developed such databases, which are made available to specialized investigators. The databases⁵⁵⁹ enable investigators to make connections between victims, abusers and places. Such databases seek to avoid duplication of effort and save time by letting investigators know whether an image or series of images have already been discovered or identified in another country, or whether an image has similar features to other images. By analysing the digital, visual and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to locate victims of child sexual abuse.

Example: UK Child Abuse Image Database

The Child Abuse Image Database (CAID) in the UK is intended to make investigating online child exploitation and abuse cases faster and more effective. It brings together all the images that the Police and National Crime Agency encounter. Regional police forces can use the images' unique identifiers – called hashes – and metadata to

improve how they investigate these crimes and protect children.

When a device is seized with indecent images of children, software allows those images to be compared with those already on the CAID database.

Using CAID reduces the need for officers or prosecutors to view large numbers of images, to see if the picture (and the child) is already known to them, saving time and avoiding unnecessary distress.

Having compared the images on the suspect's device(s) with those stored on CAID, investigators provide prosecutors with a streamlined forensic report which gives the total number of CAID-recognized images.

There may be images which have not been recognized by CAID, but which may nevertheless be indecent images of children. These images will need to be viewed separately by the police who will provide a summary of them. Such images will be added to the database.

Using a hash database, as these databases are known, reduces the impact of seeing such images on law enforcement personnel. Further, if the image possessed or distributed by the offender matches

a known image on the Interpol or other database, this can eliminate the need to produce the image in court for there to be a conviction: the fact that the images (hashes) match means that it can be

accepted as constituting child sexual abuse material. This also saves the judge and any lay adjudicators or a jury from needing to see distressing material.

Legislation **should** set out rules on the admissibility of digital and forensic evidence

Digital data is different to traditional evidence (i.e., written documents or seized items, such as a weapon or stolen goods). Before a digital device or digital content can be introduced in court as evidence, most States will require that it is authenticated (i.e., it must be shown that the evidence is what it purports to be).

Some countries require that digital evidence and traditional evidence are all authenticated in the same way, while others have specific rules relating to digital evidence. Prosecutors will need to be able to show the process, methods and tools used to collect, acquire, preserve and analyse digital evidence to show the court that the evidence was not modified in any way. This is best done in Guidelines that comply with national legislation.

Example: UNODC, E4J University Module Series on Cybercrime

To illustrate authentication practices, consider the following general categories of digital evidence: content generated by one or more persons (e.g., text, email or instant messages, and word processing documents, such as Microsoft Word); content generated by a computer or digital device without user input (e.g., data logs), which is considered as a form of real evidence; and content generated by a combination of both (e.g., spreadsheets from programmes such as Microsoft Excel, which include user input data and calculations made by the software).⁵⁶⁰

- User-generated content can be admitted if it is trustworthy and reliable (i.e., it can be attributed to a person).
- Device-generated content can be admitted if it can be shown to function properly at the time the data was produced, and if it can be shown that when data was generated security mechanisms were present to prevent the alteration of data.
- When content is both generated by a device and user, the trustworthiness and reliability of each needs to be established.

Issues of admissibility will also arise where evidence was obtained by covert means. This will require the prosecution to show that all required authorities were obtained.

- ✓ If national legislation permits the investigator to engage in unlawful activity during the course of undercover operations (see above), drafters should ensure that a further provision is added permitting the admissibility of such evidence in court.

Example: Queensland, Australia



The Police Powers and Responsibilities Act 2000, Queensland, Australia.

Article 226: Admissibility of evidence obtained through controlled activities

It is declared that evidence gathered because of a controlled activity is not inadmissible only because it was obtained by a person while engaging in an unlawful act if the unlawful act was authorized under this chapter.

8.4 Mutual legal assistance

Mutual (legal) assistance or ‘MLA’ refers to the *‘process by which States seek for and provide assistance to other States in servicing of judicial document[s] and gathering evidence for use in criminal cases’*.⁵⁶¹ Like extradition, MLA regimes are usually governed by (i) national law and (ii) bilateral or multilateral treaties.⁵⁶²

State law enforcement, criminal investigation bodies and prosecution authorities **should** cooperate and provide mutual legal assistance to equivalent bodies in other States to the widest extent possible for the purposes of investigating and prosecuting online sexual exploitation and abuse of children, including with regard to obtaining evidence, and to identifying and protecting child victims

Ensure that mutual legal assistance with another State is not conditional on the existence of a treaty for mutual legal assistance with that State

The inclusion of tailored MLA provisions in international treaties for the investigation and prosecution of online child sexual exploitation and abuse is extremely important, as *‘traditional’* MLA (and extradition) provisions were developed in the 1970s and are not tailored towards the digital environment, nor do they *‘take the volatile nature of digital crime scenes into account’*.⁵⁶³ It may take years to obtain evidence under formal MLA processes, which is too long for online child sexual exploitation and abuse, given the seriousness of the crime and possibility that the child may be at risk of ongoing harm.⁵⁶⁴ Therefore, when drafting provisions in national law for MLA, States should ensure that they have regard to the provisions on MLA in the international treaties to which they are party. These include MLA provisions in the OPSC, Lanzarote Convention, Budapest Convention and ACRWC, a summary of which is outlined below.

OPSC and OPSC Guidelines

The OPSC contains provisions concerning mutual assistance and cooperation between States parties to prevent and respond to cases of child prostitution, child pornography and the sale of

children. States parties are required to *‘afford one another the greatest measure of assistance in connection with investigations or criminal or extradition proceedings’* brought in respect of these offences, *‘including assistance in obtaining evidence at their disposal necessary for the proceedings’*.⁵⁶⁵ Further, States parties are required, subject to the provisions of its national laws, to execute requests from another State party for seizure or confiscation of goods (such as materials, assets and other instrumentalities used to commit or facilitate offences under the OPSC) and proceeds derived from such offences.⁵⁶⁶

Noting the increased use of ICT to commit or facilitate the offences covered by the OPSC, the CRC Committee has called upon States parties *‘to pay close attention to the different electronic means, including both hardware and software, used to commit such offences’* and emphasizes the need to apply OPSC measures to *‘these new ways of committing such offences, which may involve online “premises”, such as chat rooms, online forums and other online spaces that are not physical premises in the traditional sense of the term’*.⁵⁶⁷

More broadly, States parties are required to *'take all necessary steps to strengthen international cooperation by multilateral, regional and bilateral arrangements for the prevention, detection, investigation, prosecution and punishment of those responsible for acts involving the sale of children, child prostitution, child pornography and child sex tourism'*.⁵⁶⁸ Further, States parties are required to promote, among other things:

- International cooperation and coordination between their authorities, national and international non-governmental organizations and international organizations; and
- International cooperation to assist child victims in their physical and psychological recovery, social reintegration and repatriation (for which see **Part 9: Victim support, rehabilitation, reintegration and redress**).⁵⁶⁹

The OPSC Guidelines reiterate the importance of international cooperation in investigating OPSC crimes and call upon States parties to strengthen this effort and to make use of the specialized skills and resources developed by INTERPOL.⁵⁷⁰ Further, the CRC Committee calls for:

- Clear measures to strengthen the identification of victims, including through mutual legal assistance and international cooperation and INTERPOL, and to guide their rescue and repatriation, with similar means being used to identify offenders (e.g. through image analysis systems);
- Cooperation between States parties to prevent and respond to online child sexual exploitation and abuse, including through *'effective detection and reporting systems, information-sharing, and safeguarding and transmission of evidence of crimes, including electronic evidence, in a timely manner'*, as well as the provision of assistance to victims in their recovery, reintegration and repatriation, as appropriate; and
- Facilitating access by authorized actors to evidence of crimes committed across borders.⁵⁷¹

Lanzarote Convention

Article 38 concerns international cooperation to protect children from sexual exploitation and abuse, including forms facilitated by technology. Article 38(3) provides that, if a State party makes an MLA request in criminal matters conditional on the existence of a treaty and receives a request for legal assistance or extradition from a State party with which it does not have such a treaty, the former State may consider the Lanzarote Convention as the legal basis for the MLA request in criminal matters, at least with respect to offences contained in the Convention.

Budapest Convention and E-Protocol

The Budapest Convention requires States parties to cooperate and provide each other with mutual assistance *'to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'*.⁵⁷² This provision is not limited to offences under the Budapest Convention and can capture new and emerging forms of online child sexual exploitation and abuse, which may not strictly fall within the definitions of the existing offences.⁵⁷³

The MLA provisions in the Budapest Convention are contained in Articles 25 to 35. This guide does not describe each of these provisions in detail but, rather, highlights the key features which differ from the MLA provisions in the OPSC and Lanzarote Convention.⁵⁷⁴

- Articles 27 and 28 of the Budapest Convention contain procedures which apply in cases where there is an absence of a MLA agreement between a requesting or requested State party, including provisions on *'urgent'* situations. The steps include designating a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.⁵⁷⁵ However, this authority may be sidestepped in emergency situations, in which case the judicial authorities in the requesting State

may submit its request directly to the competent authorities in the requested State, copying in the central authority.⁵⁷⁶

- Article 29 generally permits a requesting State party to request another State party to order the expeditious preservation of stored data located on the requested State party's territory, while the requesting State party prepares a formal MLA request, and subject to certain exceptions, requires the requested State party to 'take all appropriate measures' to carry out the request;
- Article 30 generally provides that, if, during the course of the execution of a request made under Article 29, to preserve traffic data concerning a specific communication, the requested State party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party must 'expeditiously' disclose to the requesting party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted;
- Articles 31 to 34 contain comprehensive MLA provisions regarding investigative powers.

More generally, Article 35 requires all States parties to establish a '24/7 network' whereby each State party designates a point of contact available 24 hours a day, seven days a week, to provide 'immediate assistance' for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. The designated point of contact must have the capacity to communicate with points of contact in other State parties 'on an expedited basis', and provide a link between States parties concerning issues of international mutual assistance or extradition.

On 17 November 2021, the Committee of Ministers of the Council of Europe approved the draft '2nd Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence'.⁵⁷⁷ It will be open for signature and ratification on 12 May 2022. This Protocol, which is commonly known as the 'E-Protocol', aims to facilitate more effective investigations of cybercrimes, including cross-border investigations,

by (among other things) using 'innovative tools' to obtain the disclosure of electronic evidence.⁵⁷⁸

Enhanced cooperation provisions include provisions on 'emergency mutual assistance'.⁵⁷⁹ An emergency is defined as 'a situation in which there is a significant and imminent risk to the life or safety of any natural person'⁵⁸⁰ and includes, according to the Explanatory Report, 'ongoing sexual abuse of a child'.⁵⁸¹ The E-Protocol also contains provisions on procedures relating to international cooperation in the absence of applicable international agreements. These provisions include Article 11, under which a State party may request, and the requested State party may permit, testimony and statements to be taken from a witness or expert by video conference, including a child witness, although the requested State party 'may seek particular safeguards' with respect to child witnesses.⁵⁸²

✓ Depending on the approach to legislative drafting in the particular jurisdiction (i.e. a country where laws are short and do not contain enforcement provisions), procedural details may be more appropriately contained in secondary legislation (such as regulations, rules, directions or statutory guidelines). In such cases, the primary legislation should provide the relevant government authority with the power to issue regulations or other forms of secondary legislation. A provision should be included in the law stating that -

'the relevant authority (e.g. Minister of the leading Ministry) shall issue regulations (or other appropriate form of secondary legislation) relating to mutual legal assistance or enhanced cross-border cooperation for the investigation and prosecution of offences relating to online child sexual exploitation and abuse and the identification and protection of the child victim(s), and that such regulations should be issued within a certain period (e.g. 1 year) of the law or legal amendments coming into force'.

The delays caused by MLA should also be alleviated when the Second Additional Protocol to the Budapest Convention comes into force. The Second Additional Protocol will allow State parties, where criminal investigations and proceedings are involved, to:

(a) issue a request to an entity providing domain name registration services in the territory of another party in order to identify or contact the registrant (Article 6);

(b) issue an order to be submitted directly to a service provider in the territory of another State party to obtain the disclosure of specified, stored, subscriber information in that service provider's possession or control where the subscriber information is needed for the issuing party's specific criminal investigations or proceedings (Article 8).

An alternative mechanism for obtaining a quicker release of data is to be found in the USA's Clarifying Lawful Overseas use of Data (Cloud) Act 2018. Many ISPs are based in the USA. As noted above, due to privacy laws, the only mechanism for a State to obtain information from an ISP based in the USA, even where it relates to one of the State's own nationals, is to make a MLA request to the USA which can take up to a year to process, due to the number of requests made. In an attempt to increase the speed of application, the Cloud Act allows States with '*robust protections for privacy and civil liberties*' to enter into executive agreements with the USA to use its own laws to access electronic evidence in order to obtain information relating to the prevention, detection, investigation or prosecution of serious crime. Where there is a bilateral agreement under the Act with the USA, that State can now make an application to hand over data stored or processed by ISPs. The data covered includes the contents of communications, non-content information associated with such communications, subscriber information and data stored remotely on behalf of a user (in "the cloud").

Mutual Legal Assistance will remain a mechanism by which data can be obtained from an ISP, but the USA anticipates that the number of requests will

reduce significantly as a result of CLOUD and that consequently, requests will be processed more quickly.

Note: the legal process issued by a country under a CLOUD Agreement does not have to conform to the requirements of US Law. Instead, the legal process must conform to the requirements of the requesting country's domestic law for the data sought.⁵⁸³ The UK⁵⁸⁴ and Australia⁵⁸⁵ have reached agreement with the USA under the CLOUD Act and the European Union are currently negotiating an agreement.

- ✓ States should consider ratifying the Second Additional Protocol to the Budapest Convention as a matter of urgency.
- ✓ States should consider reaching an executive agreement with the USA under the CLOUD Act but should note that they may need to introduce legislation to ensure that they meet the '*robust protection of privacy and civil liberties*' required by the USA.

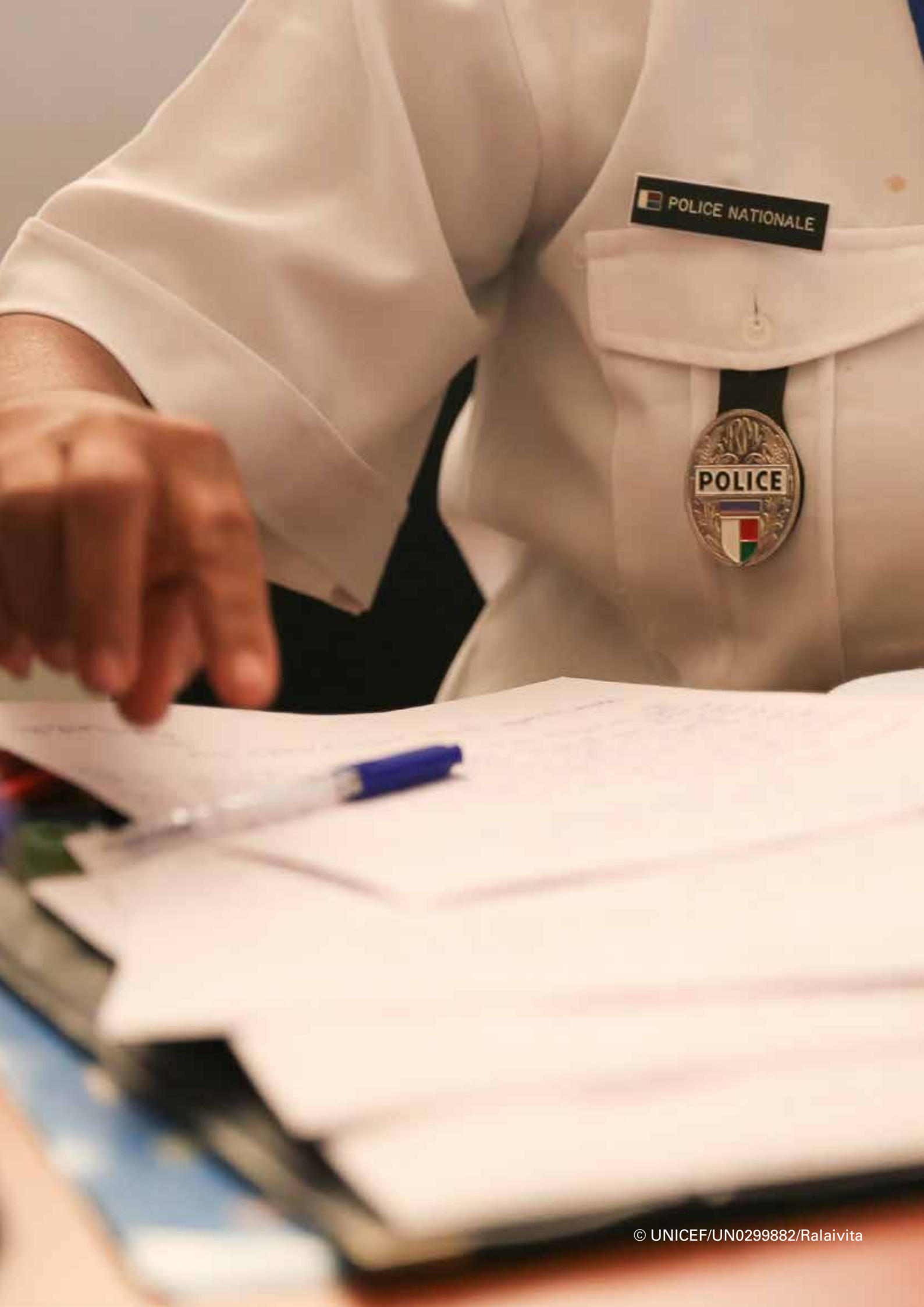


The UN issued a Proposal to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes in February 2022.⁵⁸⁶ The elements the proposal seeks to include within a new Convention include: imposing obligations on States parties to establish sufficient procedural powers to enable timely responses, investigation and prosecution of offences which are to be set out in the Convention; promoting and facilitating international cooperation, in particular through effective and rapid mutual legal assistance and the establishment of 24/7 contact points, as well as extradition, special investigative techniques and law enforcement cooperation.

Endnotes

- 519 There are 66 State parties to the Budapest Convention: Council of Europe, Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY, <<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>>.
- 520 Council of Europe Convention on Cybercrime, 2001, Article 35.
- 521 Including Australia, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Israel, Japan, Mauritius, Morocco, Panama, Paraguay, Peru, Philippines, Senegal, Sri Lanka, Tonga, and the USA.
- 522 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response, 2016, <<https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf>>
- 523 UK National Crime Agency, Virtual Global Taskforce, <<https://national-crimeagency.gov.uk/virtualglobal-taskforce/>>, accessed 24 May 2022.
- 524 For more information, see <<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/child-sexual-abuse-and-exploitation>>
- 525 The Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, <<https://asean.org/wp-content/uploads/2021/01/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf>>
- 525 OCEANZ, <www.police.govt.nz/advice-services/cybercrime-and-internet/online-child-safety>, accessed 6 April 2022.
- 527 Ibid.
- 528 The official portal of Royal Malaysia Police (n.d.), Jabatan Siasatan Jenayah. The D11 Division is also in charge of developing and coordinating nationwide prevention campaigns, training programmes and ensuring that adequate facilities are available for children. Chin. E.S.M. (2018, February 9). After four years polices anti-child sexual crimes unit officially launched. MalayMail; UN Human Rights Council (2019, January 17). Visit to Malaysia - Report of the Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse, A/HRC/40/51/Add/3.
- 529 IACAT, IJM, Online Sexual Exploitation of Children in the Philippines, <www.ijm.org/vawc/blog/osec-study, accessed 24 May 2022; UNICEF, Child Protection in the Digital Age, 2016, <www.unicef.org/eap/reports/child-protection-digital-age>; and Speller E., Protection against Child Sexual Exploitation and Abuse in the Commonwealth: Research Mapping Report (undated), <<https://itsapenalty.org/wp-content/uploads/2020/03/ET-CSEA-Legislation-in-Commonwealth-Research-Mapping-Report.pdf>>
- 530 Budapest Convention, Article 14.1
- 531 Article 3.2 of the OPSC requires States parties, subject to the provisions of their national laws, to criminalize attempts of, and complicity or participation in offences contained in the OPSC.
- 532 Harfield, C, Undercover policing – a legal-comparative perspective, In (Ed) De Boer M., Comparative Policing from a Legal Perspective, Elgar, 2018, DOI: 10.4337/9781785369117.00015
- 533 HMICS, Strategic Review of Scotland's response to online child sexual abuse, February 2020, para. 199.
- 534 From the Draft Report on the Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 2018/0108 (COD), <www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf>, accessed 6 April 2022.
- 535 Ghana, Cyber Security Act 2020, para. 97.
- 536 Whittle, Helen, et al., 'Victims' Voices: The Impact of Online Grooming and Sexual Abuse', Universal Journal of Psychology, vol. 1, no. 2, 2013, pp. 59-71, <<http://www.hrpub.org/download/201308/ujp.2013.010206.pdf>>. See also, Gregor Urbas, 'Protecting Children from Online Predators: The Use of Covert Investigation Techniques by Law Enforcement', University of Canberra, Journal of Contemporary Criminal Justice, vol. 26, no. 4, 2010, pp. 410-425 (on file with the International Centre for Missing and Exploited Children).
- 537 UN Committee on the Rights of the Child, General Comment 25, CRC/C/GC/25, 2 March 2021, para. 47.
- 538 See ICRC, International Rules and Standards for Policing, 2015, <<https://www.icrc.org/en/doc/assets/files/other/icrc-002-0809.pdf>> and Murdoch L., and Roche R., The European Convention on Human Rights and Policing, Council of Europe, 2013, <https://www.echr.coe.int/documents/handbook_european_convention_police_eng.pdf>.
- 539 ICMEC, Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review, 1st Edition, 2017, pp. 28-30.
- 540 Bleakely, Paul, 'Watching the Watchers: Taskforce Argos and the evidentiary issues involved with investigating the Dark Web child exploitation networks', The Police Journal: Theory, Practice and Principles, vol. 92, no. 3, 2019, pp. 221-236. See also, Witting S., Child Sexual Abuse in the Digital Era: Rethinking legal frameworks and transitional law enforcement collaboration, November 2020, <<https://scholarlypublications.universiteitleiden.nl/access/item%3A2966712/view>> for some of the problems in permitting investigative bodies to commit criminal acts, and see section § 110d of the German Criminal Procedure Act. <https://www.gesetze-im-internet.de/stpo/_110d.html>.
- 541 Kimmins J. P., Report of the Inquiry into allegations of Misconduct in the Investigation of Paedophilia in Queensland, Brisbane, Criminal Justice Commission, 1998.
- 542 Bleakely Paul, 'Watching the Watchers: Taskforce Argos and the evidentiary issues involved with investigating the Dark Web child exploitation networks', The Police Journal: Theory, Practice and Principles, vol. 92, no. 3, 2019, pp. 221-236.
- 543 The Organic Integral Criminal Code of Ecuador 2014, <[https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/ImplementingLaws.xsp?documentId=D6FE6928F486E375C1257E58004B3102&action=openDocument&xp_countrySelected=EC&xp_topicSelected=G-VAL-992BU6&from=state#:~:text=On%2028%20January%202021](https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/ImplementingLaws.xsp?documentId=D6FE6928F486E375C1257E58004B3102&action=openDocument&xp_countrySelected=EC&xp_topicSelected=G-VAL-992BU6&from=state#:~:text=On%2028%20January%202021.)>. See Articles 475-477, related to the Retention of Correspondence, including the electronic sort; the Interception of Computer-based Communications or Data regarding sending and recording of computer data in transit through telecommunications services, and recognition of recordings.
- 544 UK Child Prosecution Service, Guidance on Online Child Abuse Activist groups on the internet, July 2020, <www.cps.gov.uk/legal-guidance/online-child-abuse-activist-groups-internet>, accessed 6 April 2022.
- 545 Australia Centre to Counter Child Exploitation, Blueprint 2019-2021.
- 546 Optional Protocol to the Convention on the Rights of the Child, Article 7.
- 547 Lanzarote Convention, Article 27(2) and Budapest Convention, Article 19.
- 548 The Commonwealth consists of 54 countries which largely adhere to the common law system. The Commonwealth Office of Civil and Criminal Justice Reform, Model Law on Computer and Computer Related Crime 2017, <www.thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf>, accessed 10 November 2021.
- 549 Model Law, Section 11.
- 550 See also the Budapest Convention Article 19(3) which contains similar provisions.
- 551 The Supreme Court of the Philippines has issued a Rule on Cybercrime Warrants that further clarifies the types and specific requirements of cybercrime warrants that law enforcement can apply for. <<https://sc.judiciary.gov.ph/1420/>>
- 552 See UNODC, Handling of digital evidence, <<https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html>>
- 553 Based on information from key informant interviews.

- 554 Model Law on Computer and Computer Related Crime, <[production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf](#)> accessed 28 May 2022.
- 555 Maras, Marie-Helen, Computer Forensics: Cybercriminals, Laws, and Evidence. Jones and Bartlett, 2014.
- 556 Key informant interviewees with Australian Federal Police.
- 557 Association of Chief Police Officers (ACPO), now the National Police Chiefs Council (UK), Guidelines for Handling Digital Evidence, https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf; The National Institute of Standards and Technology of the United States Department of Commerce and the Scientific Working Group on Digital Evidence are other sources of best practices, technical notes and guidelines for forensic quality and consistency. See also Real Time Networks, <https://www.realtimenet-works.com/blog/preserving-digital-evidence-the-right-way-your-10-step-guide>
- 558 International Child Sexual Exploitation Database, <<https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database>>
- 559 The databases contain PhotoDNA, also known as image hashing; a technology developed by Microsoft which takes known images, breaks them down into pieces, and assigns a unique hash sequence to the image. The image hash is added to a database and then, based on that database, already identified images can be picked up again when they are uploaded to a platform that has the PhotoDNA screening capability.
- 560 UNODC, University Module Series: Cybercrime, <<https://www.unodc.org/e4j/en/tertiary/cybercrime.html>> , accessed 28 May 2022.
- 561 UNODC, University Module Services, Module 11: International Cooperation to Combat Transnational Organized Crime, Mutual Legal Assistance, <www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html>, accessed 9 December 2021.
- 562 Witting, S.K., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', The International Journal of Children's Rights, vol. 29, 2021, pp. 731-764, p. 746.
- 563 Ibid.
- 564 Ibid.
- 565 OPSC, Article 6.1.
- 566 Ibid., Article 7(b).
- 567 OPSC Guidelines, para. 75.
- 568 OPSC, Article 10.1.
- 569 OPSC, Article 10.1 and 10.2.
- 570 OPSC Guidelines, para. 81.
- 571 Ibid., paras. 76, 81, 101, 109 and 112.
- 572 Budapest Convention, Articles 23 and 25.1.
- 573 Witting, S.K., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', The International Journal of Children's Rights, vol. 29, 2021, pp. 731-764, p. 750.
- 574 As highlighted by Witting, S.K., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', The International Journal of Children's Rights, vol. 29, 2021, pp. 731-764, p. 751.
- 575 Budapest Convention, Article 2(a).
- 576 Ibid., Article 9(a).
- 577 Council of Europe, Protocol Negotiations, <www.coe.int/en/web/cybercrime/t-cy-drafting-group>, accessed 14 February 2022.
- 578 Council of Europe, E-evidence Protocol approved by Cybercrime Convention Committee, Strasbourg, 31 May 2021, https://www.coe.int/en/web/human-rights-rule-of-law/events/-/asset_publisher/E5WWthsy4Jfg/content/e-evidence-protocol-approved-by-cyber-crime-convention-committee?_101_INSTANCE_E5WWthsy4Jfg_view_Mode=view/ accessed 24 May 2022, and https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d accessed 12 May 2022. See also, <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/CRPs/V2201067.pdf>.
- 579 2nd Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (E-Protocol), Strasbourg, 12.V.2022, Article 10, https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d accessed 12 May 2022.
- 580 E-Protocol, Strasbourg, 12.V.2022, Article 3.2(c), https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d, accessed 12 May 2022.
- 581 Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, Strasbourg, 12.V.2022, para. 42, https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b, accessed 12 May 2022.
- 582 Ibid.
- 583 Purpose of the Cloud Act, <www.justice.gov/dag/page/file/1153466/download>
- 584 On 8 July 2020, the bilateral agreement between the USA and the UK on Access to Electronic Data for the Purpose of Countering Serious Crime entered into force; United States Department of Justice, Office of the Assistant Attorney General, Letter dated 16 January 2020, <https://www.justice.gov/dag/page/file/1236281/download>, accessed 19 May 2022. See generally Lostri E., The CLOUD Act, Center for Strategic and International Studies, 2 October 2020, <https://www.csis.org/blogs/technology-policy-blog/cloud-act>, accessed 19 May 2020.
- 585 The Australian government introduced the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, which would allow them to enter into 'bilateral and multilateral agreements for cross-border access to electronic information and communications data'; Telecommunications Legislation Amendment (International Production Orders) Bill 2020, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6511_first-reps/toc_pdf/20025b01.pdf;fileType=application%2Fpdf, accessed 19 May 2022; Explanatory Memorandum, para. 7, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6511_ems_0ac5ae09-3e3e-400b-ae5e-680a68af4e45/upload_pdf/733176.pdf;fileType=application%2Fpdf, accessed 19 May 2022.
- 586 A/AC.291/CRP/8, 24 February 2022, <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/CRPs/V2201067.pdf>.



9. Victim support, rehabilitation, reintegration and redress

Checklist of minimum and recommended standards

Ensure child friendly practices and support are applied to child victims and witnesses in the justice system

Rehabilitation and reintegration services **should** be strengthened to address the unique needs of child victims of online sexual abuse and exploitation

Services to prevent further victimization **should** be available to child victims and their families

Ensure specialist training on the digital context is provided to the workforce that responds to child victims of sexual abuse and exploitation

Collaboration and coordination between the different stakeholders involved in child sexual exploitation cases and child protection services **should** be formalized

Measures that ensure sufficient financial resources are allocated annually to victim support services **should** be introduced

Consider establishing a helpline that provides detailed information and referrals to the relevant service provider

Consider establishing clear procedures for the swift removal of child sexual abuse materials

Differing forms of and platforms for compensation **should** be offered to child victims

9.1 Detail of minimum and recommended standards

Ensure child friendly practices and support are provided to victims and witnesses in the justice system

It is a well-established principle within international and regional law that special consideration should be provided to child victims and witnesses during criminal proceedings, which they can find intimidating. This is particularly true in cases of online sexual abuse of a child, due to the complicated nature of the offence and its associated processes.

International standards

Article 8.3 of the OPSC states that *'in the treatment by the criminal justice system of children who are victims of the offences described in the present Protocol, the best interest of the child shall be a primary consideration.'* This is reiterated in the OPSC Guidelines, where the Committee reminds States parties of their *'obligation to provide appropriate support and legal counselling to assist child victims of offences covered in the Optional Protocol at*

*all stages of criminal justice proceedings and protect their rights and interests, and to ensure that the best interests of the child is a primary consideration.*⁵⁸⁷ The Committee recommends that States parties refer to the Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime⁵⁸⁸ which sets out good practice that States should follow to ensure that children are able to give evidence in the prosecution of their abuser. The Guidelines provide that: *'Child victims and witnesses should be treated in a caring and sensitive manner throughout the justice process.'*⁵⁸⁹ A child victim's interests should therefore be treated as paramount during the judicial process, and appropriate support should be provided.

The nature of online crimes, and the many stakeholders involved with obtaining evidence relating to the offence, means that judicial processes can be lengthy and complicated. The major issues for child victims of all forms of sexual exploitation and abuse are delay and the stress of giving evidence in court when a trial finally takes place. There are a number of measures that can be introduced to address these problems. The police, prosecutors, judiciary and social workers involved in cases concerning the online sexual exploitation of a child should receive specialist training in this field, as outlined in General Comment No. 25⁵⁹⁰ and in the OPSC Guidelines.⁵⁹¹ Some cite a lack of knowledge or understanding of the crime from these professionals as a common reason for failed convictions. Keeping an open dialogue about the process with the victim is also important, as it helps reduce feelings of despair or apathy regarding the case. Social workers, prosecutors and other relevant actors should ensure that victims are fully informed about the court process as provided in Article 8 of the OPSC, which provides that States parties must inform *'child victims of their rights, their role and the scope, timing and progress of the proceedings and of the disposition of their cases'*.⁵⁹²

✓ States parties should introduce measures that allow evidence to be given by the child outside the courtroom, to reduce further trauma. In the OPSC Guidelines, the Committee recommends *'that the child's testimony be taken under conditions of due process outside the court room'*⁵⁹³ and where

possible *'appropriate communication technology'* should be used to *'enable child victims to be heard during the trial without being present in the courtroom. This becomes essential in judicial proceedings involving Optional Protocol offences committed against children abroad, to enable testimonies from victims in other countries.'*⁵⁹⁴ This can be done either by video live-link at the trial itself, so the victim does not need to be in same room as the defendant, or through pre-recorded video evidence.⁵⁹⁵ The advantage of pre-recorded video evidence, taken after charges have been filed against the defendant, and standing in place of the child giving oral evidence at a trial, is that the child can move on with the process of rehabilitation and reintegration and is not affected by the delays of the criminal justice system.

Example: Brazil



In 2017, Brazil adopted Law No. 13.431⁵⁹⁶ on establishing a system for guaranteeing the rights of children and adolescents who are victims or witnesses of violence, with specific reference to online sexual violence. The Law includes provisions on specialized procedures for interviewing children and adolescents and for taking their testimony before police or judicial authorities. The provisions are intended to, among other things, protect the child from revictimization and trauma, facilitate their right to be heard, protect their privacy, preserve their dignity and obtain the best possible evidence for criminal proceedings.

'Art. 4 For the purposes of this Law, without prejudice to the classification of criminal conduct, the following are forms of violence:.....

III - sexual violence, understood as any conduct that compels a child or adolescent to practice or witness carnal intercourse or any other lewd act, including exposure of the body in photo or video electronically or otherwise, which includes:

a) sexual abuse, understood as any action that uses the child or adolescent for sexual purposes,

whether sexual intercourse or other lewd acts, carried out in person or by electronic means, for sexual stimulation of the agent or a third party;

b) commercial sexual exploitation, understood as the use of a child or adolescent in sexual activity in exchange for remuneration or any other form of compensation, independently or under the sponsorship, support or encouragement of a third party, either in person or by electronic means;

c) trafficking in persons, understood as the recruitment, transport, transfer, housing or reception of children or adolescents, within the national territory or abroad, for the purpose of sexual exploitation, through threat, use of force or any other form of coercion, kidnapping, fraud, deception, abuse of authority, taking advantage of a situation of vulnerability or delivery or acceptance of payment, among the cases provided for in the legislation;

.....

Art. 7 Specialized listening is the procedure of interviewing a situation of violence against a child or adolescent before an organ of the protection network, limiting the report strictly to what is necessary for the fulfilment of its purpose.

Art. 8 Special Testimony is the procedure for hearing a child or adolescent victim or witness of violence before police or judicial authorities.

Art. 9 The child or adolescent will be protected from any contact, even visual, with the alleged perpetrator or accused, or with another person that represents a threat, coercion or embarrassment.

Art. 10. Specialized listening and special testimony will be carried out in an appropriate and welcoming place, with infrastructure and physical space that guarantee the privacy of the child or adolescent victim or witness of violence.

Art. 11. The special testimony will be governed by protocols and, whenever possible, will be carried out only once, in the seat of anticipated

production of judicial evidence, guaranteeing the full defense of the investigated.

§ 1 The special testimony will follow the precautionary rite of anticipation of evidence:

- when the child or adolescent is less than 7 (seven) years old;

II - in case of sexual violence.

§ 2° The taking of a new special testimony will not be allowed, except when justified its indispensability by the competent authority and there is the agreement of the victim or the witness, or their legal representative.

Art. 12. The special testimony will be collected according to the following procedure:

I - the specialized professionals will clarify the child or adolescent about the taking of the special statement, informing them of their rights and the procedures to be adopted and planning their participation, being prohibited the reading of the complaint or other procedural documents;

II - the child or adolescent is assured a free narrative about the situation of violence, and the specialized professional can intervene when necessary, using techniques that allow the elucidation of the facts;

III - in the course of the judicial process, the special testimony will be transmitted in real time to the hearing room, preserving confidentiality;

IV - once the procedure provided for in item II of this article is concluded, the judge, after consulting the Public Prosecutor's Office, the defender and the technical assistants, will assess the pertinence of supplementary questions, organized as a block;

V - the specialized professional will be able to adapt the questions to the language of better understanding of the child or adolescent;

VI - the special testimony will be recorded in audio and video.

§ 1 The victim or witness of violence is guaranteed the right to testify directly to the judge, if he/she so wishes.

§ 2 The judge will take all appropriate measures to preserve the intimacy and privacy of the victim or witness.

§ 3 The specialized professional shall inform the judge if he or she finds that the presence, in the courtroom, of the perpetrator of the violence may harm the special testimony or put the deponent at risk, in which case, stating in a term, the removal of the accused will be authorized.

§ 4 In cases where there is a risk to the life or physical integrity of the victim or witness, the judge will take the appropriate protection measures, including the restriction of the provisions of items III and VI of this article.

§ 5 The conditions of preservation and security of the media related to the testimony of the child or adolescent will be the object of regulation, in order to guarantee the right to intimacy and privacy of the victim or witness.

§ 6 The special testimony will be processed in judicial secrecy.⁵⁹⁷

Rehabilitation and reintegration services **should** be strengthened to address the unique needs of child victims of online sexual abuse and exploitation

Child sexual abuse and exploitation have numerous adverse effects on a victim's mental, emotional and physical health and development. The particularities of child sexual exploitation and abuse with an online or digital dimension can bring about additional or different impacts. Some documented effects include physical harms, insomnia, educational delay, psychological distress and isolation, self-destructive behaviour such as substance abuse and, in extreme cases, suicide.⁵⁹⁸ Appropriate victim support, rehabilitation and reintegration services, as well as receiving redress for abuse are therefore key to the recovery of victims of all forms of child sexual exploitation and abuse. The existence of a robust end-to-end support system with expertise to deal with the specificities of the online dimensions is a key element in tackling the short and long-term consequences of being subject to child sexual abuse and exploitation.

International standards

Article 39 of the CRC requires State parties to adopt measures that promote the *'physical and psychological recovery and social reintegration of a child victim'*, and this must take place *'in an*

environment [that] fosters the health, self-respect and dignity of the child'. This is reflected in OPSC Article 9.3 which provides that *'States Parties shall take all feasible measures with the aim of ensuring all appropriate assistance to victims ... including their full social reintegration and their full physical and psychological recovery'*. The OPSC Guidelines go further: *'It is crucial, through legislation, to secure the availability of child- and gender-sensitive, confidential and safe counselling, to address incidents of sexual exploitation and sexual abuse and protect victims'*.⁵⁹⁹

General Comment No. 25 notes that specialized protections may be required to *'redress harms associated with the digital environment'*.⁶⁰⁰ There may be a difference in terms of the impact and trauma suffered in online as compared to offline sexual abuse cases. For example, the continued existence and circulation of a child's image online may *'impact the recovery and reintegration process and may increase the need for long-term psychological counselling and social services'*.⁶⁰¹ The OPSC Guidelines have recognized this and call for States parties to adopt *'adequate measures to provide long-term social and psychological services*

as needed'.⁶⁰² The OPSC Guidelines also encourage States parties to give 'specific consideration' to children marginalized by their contexts, explicitly referring to gender identities, children with disabilities, migrant children, among others.⁶⁰³

The CRC Committee General Comment No. 25 (2021) reflects the approach taken in the OPSC Guidelines and recommends that States parties 'establish, coordinate and regularly monitor and evaluate frameworks for ... the provision of effective support to children who are victims'.⁶⁰⁴ This framework should include 'multiagency and child-friendly' measures that facilitate the 'therapy and follow-up care for, and the social reintegration of children who are victims'.⁶⁰⁵

Regional standards

Although there are numerous regional frameworks that criminalize the online sexual abuse of children, few have addressed the state obligation to provide victim support, rehabilitation or reintegration services in depth.

One prominent regional law that has addressed this issue is the Council of Europe's Lanzarote Convention. The Convention outlines how States parties should offer and ensure access to support services that facilitate a child victim's physical and psychological recovery, social reintegration, and prevent their re-victimization. In 2017, the Lanzarote Committee clarified that despite not explicitly referring to ICTs, everything criminalized in the Convention extends to the context of the digital space.⁶⁰⁶ The Committee also recommended that 'in addition to the actual damage caused to the victim, due attention should be paid to the specific long-term impact that sexual offences against children facilitated through the use of ICTs can have on the victims', considering that the relevant image may continue to be circulated after the abuse has occurred.⁶⁰⁷

The Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN also outlines the need to increase the 'effectiveness of rights-based and gender-responsive

child protection and support services, social welfare programmes'.⁶⁰⁸

Example: Republic of Korea

In April 2018, the Ministry of Gender Equality and Family in the Republic of Korea established the Digital Sexual Crime Victim Support Center (DSCVSC). The Center offers 'comprehensive services such as counselling, deleting support, investigative support, litigation support, and post-monitoring' in support of cases concerning online sexual abuse and exploitation. The Center also provides financial assistance for medical expenses and collects data concerning digital sexual abuse crimes in Korea, which helps inform future action and service provision.⁶⁰⁹

- ✓ States should ensure that legislation provides for support services for children who are victims of all forms of sexual exploitation and abuse, including those with an online dimension. Such services should be child friendly and multidisciplinary and preferably available at one-stop centres, in which all the different actors intervening for the child's care and protection are present, including therapeutic and medical services. Such centres should offer multidisciplinary and inter-agency collaboration to ensure that child victims and witnesses benefit from a child- and gender-sensitive, professional and effective response in a safe environment, preserving their best interests at all times.⁶¹⁰
- ✓ Legislation must ensure that access to support services is not dependent on a child's participation in any proceedings related to the offence.

Services to prevent further victimization **should** be available to child victims and their families

The OPSC Guidelines recommend that States develop a comprehensive continuum of care and support⁶¹¹ for the child victim, including post-trial reintegration services to help limit the trauma caused by their abuse, as well as prevent revictimization.

In most cases, the child's parents and family will play a crucial role in providing support to a child who has been the victim of online sexual exploitation and abuse. The family may, however, also need support in terms of learning the best way to help, how to protect the child from further exploitation and abuse and how to deal with any secondary trauma they may have experienced themselves as a result of learning about their child's abuse. This is particularly important in cases where the abuser was another family member.⁶¹²

There is a danger that the risk factors that initially made the child vulnerable to abuse continue to exist. This is the case even where the parents were not culpable in the child's exploitation or abuse. Such risk factors include, but are not limited to, whether the abuser is closely associated with the child or family, the victim's familial dynamics and home structure, their financial situation, as well as their educational development.⁶¹³ Monitoring the potential risk factors a child may face at home, while also ensuring that familial systems have the capacity to care for the victim, will help facilitate the victim's successful reintegration.

✓ Legislation requiring the provision of support services for child victims of sexual exploitation and abuse should include assessment of ongoing risk and support to families to manage such risk.

Ensure specialist training on the digital context is provided to the workforce that responds to child victims of sexual abuse and exploitation

The manner in which a victim is dealt with by professionals is highly likely to influence the extent to which a victim engages with the rehabilitation or re-integration process,⁶¹⁴ thus affecting their recovery. States should ensure that those handling cases of sexual exploitation and abuse (i.e., social workers, health professionals, law enforcement, prosecutors) receive specialist training to enable them to deal with such cases in an appropriate manner.

This obligation is enshrined in Article 8.4 of the OPSC, which outlines that '*States Parties shall take measures to ensure appropriate training, in particular legal and psychological training, for the persons who work with victims of the offences prohibited under the present Protocol*'. General Comment No. 25 also outlines how States parties should '*provide specialized training for law enforcement officials, prosecutors and judges regarding child rights violations specifically*

associated with the digital environment'⁶¹⁵ and '*professionals working for and with children and the business sector, including the technology industry, should receive training that includes how the digital environment affects the rights of the child in multiple contexts, the ways in which children exercise their rights in the digital environment and how they access and use technologies*'.⁶¹⁶

The UN Economic Social Council's Guidelines on Justice in Matters involving Child Victims and Witnesses recommends that adequate training should be made available to professionals working with child victims, so that they can deal with them in an effective and sensitive manner.⁶¹⁷ The guidelines recommend that this training should include:

- a. Relevant human rights norms, standards and principles, including the rights of the child;
- b. Principles and ethical duties of their office;
- c. Signs and symptoms that indicate crimes against children;
- d. Crisis assessment skills and techniques, especially for making referrals, with an emphasis placed on the need for confidentiality;
- e. Impact, consequences, including negative physical and psychological effects, and trauma of crimes against children;
- f. Special measures and techniques to assist child victims and witnesses in the justice process;
- g. Cross-cultural and age-related linguistic, religious, social and gender issues;
- h. Appropriate adult-child communication skills;
- i. Interviewing and assessment techniques that minimize any trauma to the child while maximizing the quality of information received from the child;
- j. Skills to deal with child victims and witnesses in a sensitive, understanding, constructive and reassuring manner;
- k. Methods to protect and present evidence and to question child witnesses;
- l. Roles of, and methods used by, professionals working with child victims and witnesses.⁶¹⁸

Having a knowledgeable and sensitive workforce means professionals can offer the appropriate support child victims need while going through criminal investigations, legal proceedings and the recovery process. While States may have an existing workforce that is trained in responding to cases of child sexual abuse, tailored training should be provided on how to identify and handle cases in the digital environment. Educating the workforce about online sexual abuse and exploitation, the myths and the realities surrounding the crime, as well as the laws, services and procedures in place to tackle it, will enable them to handle such cases with confidence and expertise and in a trauma-informed manner. Providing specialized training to the workforce would help ensure that considerations for the digital context are integrated across the child protection system as a whole.

✓ Legislation should set out the required training to be undergone by professionals working with child victims of all forms of sexual exploitation and abuse, including those facilitated by technology.

Collaboration and co-ordination between the different stakeholders involved in online sexual exploitation cases **should** be formalized

Many actors and agencies are involved when a case concerning the online sexual exploitation or abuse of a child is referred or investigated, including law enforcement, social services and children's services. Collaboration between different bodies and agencies is encouraged under General Comment No. 25 (2021), which outlines how frameworks and services provided to child victims should be 'multiagency and child-friendly'.⁶¹⁹

ECOSOC Resolution 2005/20 also recommends that professionals 'make every effort to adopt an interdisciplinary and cooperative approach in aiding children by familiarizing themselves with the wide array of available services, such as victim support, advocacy, economic assistance, counselling, education, health, legal and social services. This approach may include protocols for the different stages of the justice process to encourage cooperation among entities that provide services to child victims and witnesses, as well as other forms of multidisciplinary work that includes police, prosecutor, medical, social services and psychological personnel'.⁶²⁰

Collaboration may be relatively low level, involving information sharing, the exchange of resources, or simply referral between the services. There are, however, advantages to joint working between agencies, professionals or services. For example, the WeProtect Model National Response Framework recommends that States consider embedding social workers within law enforcement units dealing with child sexual exploitation and abuse investigations, because it ensures that child protection needs are prioritized throughout the process.⁶²¹

Example: Republic of the Philippines

The Philippine's Department of Justice Protocol for Case Management of Child Victims of Abuse, Neglect, and Exploitation promotes a multi-sectoral approach when dealing with cases of child sexual abuse. It recognizes that children 'need access to an array of services due to the multi-faceted nature of their needs' and requires agencies and professionals to work together to provide victims with the appropriate protection, and legal and social services they need.

This multi-sectoral approach entails clear collaboration between national and local government agencies, NGOs, faith-based organizations, civic organizations, the private sector, police, prosecutors, judges, lawyers, social workers, medical doctors, psychiatrists, psychologists and other officials. The roles and responsibilities of the differing actors are outlined in the protocol, starting from the reporting or referral of the child abuse case, up until the child has been fully integrated into their families and communities. The protocol contains a flowchart explaining the order of the end-to-end support that is to be provided to child victims.

- ✓ States parties should develop standard operating procedures / joint working protocols that set out the different roles and responsibilities of the various agencies and how the different agencies are expected to work together.

Measures that ensure sufficient financial resources are allocated annually to victim support services **should** be introduced

Article 4 of the CRC places a duty on States parties to ensure they take *'all appropriate legislative, administrative, and other measures for the implementation of the rights recognized in the present Convention'*. General Comment 19 elaborates on Article 4, stating that it includes the duty to ensure *'Laws and policies are in place to support resource mobilization, budget allocation and spending to realize children's rights'*.⁶²²

The OPSC guidelines recommends that States parties *'ring-fence'* financial resources and allocate this to the entities in charge of (among others) *'the physical and psychological recovery and social reintegration of child victims'*.⁶²³ Furthermore, in line with General Comment No. 25, States parties should *'mobilize, allocate and utilize public resources to implement legislation, policies and*

programmes to fully realize children's rights in the digital environment'.⁶²⁴

Programmes and systems that provide support to victims of online sexual exploitation and abuse, and particularly specialist support services that cater to children from marginalized backgrounds,⁶²⁵ require stable, ongoing funding. Guaranteed funding ensures the consistent implementation and sustainability of programmes and services and enables providers to build up and retain professional staff.

✓ States parties should include a requirement to fund rehabilitation programmes and other support services for child victims of sexual exploitation and abuse in legislation together with a legal obligation to report on expenditure on services annually to either the relevant ministry or to the legislature.

Consider establishing a helpline that provides detailed information and referrals to the relevant service provider

Helplines are useful mechanisms for providing information on, or referrals to, the necessary service provider. Although often used interchangeably, helplines should be distinguished from hotlines. Helplines typically focus on providing general support and reintegration services, including referrals to shelters, rehabilitative services, counselling, medical services etc., while hotlines are set up to receive reports of online child sexual abuse materials and to have the materials taken down from the internet (see **Part 7: Duties and responsibilities in relation to business** for more information on notice and takedown).

The WeProtect Model National Response framework sets out the key elements for a child-friendly helpline:

- Confidential and anonymous;
- Accessible free of charge;
- Open 24 hours per day, seven days a week;
- Operated through means other than just telephone i.e. text messaging, internet chat services/internet messaging, discussion forums, email and face-to-face meetings; and
- Operated in partnership with key referral services i.e. educational facilities, hospitals, shelters and other child-related services.⁶²⁶

Example: Bangladesh

Bangladesh maintains two helplines. First, a toll-free Child Help Line number, “1098”, which is implemented by the Department of Social Services under the Ministry of Social Welfare and is funded by the telecommunications conglomerate, Telenor. This 24-hour telephone line provides emergency support services to children at risk and links children with existing social protection services through rescue, safe shelter and referral. The second helpline “10921”, run by the Multi-sectoral Programme on Violence Against Women, offers legal advice, telephone counselling and information or referrals to NGOs, the police, Victim Support Centres and One-Stop Crisis Centres.⁶²⁷

Example: Republic of the Philippines

Bantay Bata 163 is the child welfare arm of ABS-CBN Lingkod Kapamilya Foundation Inc, which is the NGO subsidiary of the Filipino media conglomerate ABS-CBN. As a part of their services, they offer a toll-free national helpline that provides immediate responses to emergency child safety cases, as well as offering community and family support services, alternative care and outreach programmes. The programme also works with national and local government agencies, such as the Department of Social Welfare and Development.

When establishing a helpline, the question frequently arises as to which body should operate the helpline? Globally, a mix of bodies, including government agencies, NGOs and private sector bodies run helplines. NGOs are often the preferred operating bodies, due to their ability to collaborate effectively with public and private partners, their expertise in child protection or online safety, and their independence, which means the public may feel more secure accessing their services.⁶²⁸

States should consider establishing a network of key referral agencies to which the helpline can make referrals, to ensure the helpline is run effectively. Maintaining a single point of contact with key child protection bodies, welfare services, law

enforcement officers and key industry players, helps to ensure smooth collaboration with specialist help. Moreover, having clearly defined referral pathways, aligned with the law and data protection rules, ensures that cases are dealt with in a swift and efficient manner. Other important considerations include providing the helpline with sufficient resources and funding and publicizing the helpline so that children are aware it exists and use it when necessary.⁶²⁹

✓ It is essential that helpline staff are trained to have the capacity to deal with issues relating to the digital environment, as well as the ability to offer services in a child-sensitive manner.⁶³⁰

One of the disadvantages of NGO helplines is insecurity of funding. Such helplines rely on government and donor support, and this is often provided on a short-term basis, creating constant uncertainty about long-term funding. Integrating a legislative requirement to report on the funding and performance of support services, as was recommended in the previous standard, could encourage better resourcing, effectiveness, and help secure the long-term sustainability of NGO helplines.

General Comment No. 13 also outlines how ‘robust monitoring mechanisms must be developed and implemented to ensure accountability regarding allocation of budgets and their efficient utilization’.⁶³¹

✓ Where helplines are provided with State funding, legislation should require that the receiving body report on its performance and funding, in order to monitor whether helplines are being run efficiently.

Consider establishing clear procedures for the swift removal of child sexual abuse materials

A key priority for victims is the removal of images or videos of their abuse from the online platform(s) on which it has been shared, as the potential continued circulation of their image means they experience a constant cycle of revictimization.⁶³² General Comment No. 25 regards the *'removal of unlawful content'* as an appropriate form of reparation for harms caused.

ISPs should therefore establish robust procedures to ensure the timely removal of child sexual abuse

materials. **Part 7: Duties and responsibilities in relation to business** discusses in detail the need for notice and takedown procedures and recommends a process that can be used by ISPs to make sure that child sexual abuse materials are promptly removed from their platforms. In addition to the removal of the sexual abuse material, stopping any further recirculation of the material is also crucial. The use of image-identification technology, such as PhotoDNA or other hash databases, will prove valuable in this endeavour.

Differing forms of and platforms for compensation **should** be offered to child victims

Article 9.4 of the OPSC provides that *'State parties shall ensure that all child victims have access to adequate procedures to seek, without discrimination, compensation for damages from those legally responsible.'* In the OPSC Guidelines, the CRC Committee recommends that States parties should carefully consider which form of compensation is preferable for each child victim depending on their circumstances. Compensation could be financial, or come in other forms, such as support for education or income-generating activities.⁶³³ The CRC Committee in its later General Comment No. 25 explains that appropriate reparation for damage includes restitution, compensation and satisfaction, which can take, for instance, the form of apology, correction, removal of unlawful content or access to psychological recovery services or other measures.⁶³⁴

Out-of-court settlements as an alternative to criminal proceedings may on occasions seem attractive, but should not be encouraged. It has been reported that many cases concerning the online sexual exploitation of children have been resolved through informal *'compromises'* in which perpetrators pay child victims to avoid legal action.⁶³⁵ This is often seen as attractive to the child and the family, due to the fact that poverty is a significant risk factor for sexual exploitation. Payment to a victim to avoid criminal prosecution and/or penalties should be strongly discouraged and opposed by law enforcement, social workers, the judiciary and other relevant officials, not only for the sake of the victim but also for future potential victims.



OPSC Guidelines

Para. 110: States Parties should provide victims with the possibility to bring civil action, regardless of their economic status, including through the provision of legal aid or through the establishment of a state-operated compensation system, and ensure that they cannot be deemed ineligible due to their involvement in the offences in question. Such civil proceedings should integrate the same child- and gender-sensitive measures as those described for criminal proceedings, as appropriate.

Para. 111: To improve the chances of victims to receive compensation from convicted offenders, States Parties should enable the identification and attachment of defendants' assets early in the proceedings and amend money laundering laws to allow victims to be paid from forfeited property. Compensation measures should be enforced in line with international standards, such as article 2.3(c) of the International Covenant on Civil and Political Rights, which sets forth that States Parties must "ensure that the competent authorities shall enforce such remedies when granted".

One way a victim can obtain compensation for their abuse is through the justice system. While it is possible in many jurisdictions to pursue a civil case seeking compensation, this can take a long time and carries the potential of further trauma for the victim. Such a process can also be complex and expensive, which may put such an action out of reach for most children and their families.

✓ To address this, criminal courts should be permitted under the law to make an order for compensation whenever there is a conviction for online sexual exploitation or abuse. However, the transnational nature of such cases presents jurisdictional complexities that could be a potential barrier for children seeking compensation through this route. States should therefore consider ways to overcome these barriers within the law, such as courts being able to provide compensation to victims who are not residents such as

undocumented or irregular migrants or children that are victims of trafficking..

✓ States should make it clear in legislation that the child victim's right to compensation is not linked to any aspect of the criminal investigation, such as the child's timeliness in reporting the online exploitation or abuse, whether the child took part in the abuse or the child's level of cooperation with the investigation. Additionally, it is recommended that the compensation received should not only cover the damages caused, but also cover the fees for the legal process and any medical, rehabilitative or other abuse-related needs the child may have.

Example: United States of America



In the USA, under Subsection 2259 of Title 18 of the US Code, the main criminal code of the federal government in the United States – mandatory restitution, the compensation given to a victim of sexual abuse includes the expenses of medical services relating to physical, psychiatric, or psychological care, physical and occupational therapy or rehabilitation, transportation, legal expenses, childcare expenses, as well as other costs and losses incurred resulting from the offence.⁶³⁶

The CRC Committee⁶³⁷ has raised concern over the difficulty courts have faced in calculating the compensation a victim should receive, especially when taking into consideration the potential recirculation of child sexual abuse material, which could involve incalculable numbers of viewers and recurring harm to the child. A further issue is the enforceability of compensation or the perpetrator's failure to disburse the funds promptly.

✓ To avoid this problem, States parties should consider amending the law to ensure that funds obtained from the perpetrator are directed to satisfy compensation orders in favour of child victims before funds are distributed elsewhere.⁶³⁸

An accepted alternative to civil action in the courts is a State-managed compensation fund. These offer a more informal and accessible way of seeking redress and are an attractive alternative to the civil

justice system.⁶³⁹ Typically, compensation funds are regulated by law and are managed by a board or a government agency that examines applications and determines whether an award should be given and to what amount.⁶⁴⁰ Many States already have State-managed compensation funds in place, but these frequently limit recovery to victims of violent crimes. Sexual exploitation of children, including exploitation through child sexual abuse materials, are generally not included.⁶⁴¹

These schemes, while attractive, have to be funded and this can pose a challenge for many States. There are a range of funding models, including contributions by ISPs and other private bodies. In their 2017 Report, ECPAT examined the differing forms of compensation available to child victims of sexual abuse and found that similar barriers to seeking compensation existed globally. Such barriers included:

- The lack of notice and information regarding the right to compensation;
- The lack of legal assistance/legal aid available to children to go through the process;
- The complexity of transnational cases;
- Prescription periods, statutes of limitations and other time restrictions limiting the victim's ability to obtain compensation;
- Problems with receiving payments i.e. delayed enforcement or irresponsible management from guardian.⁶⁴²

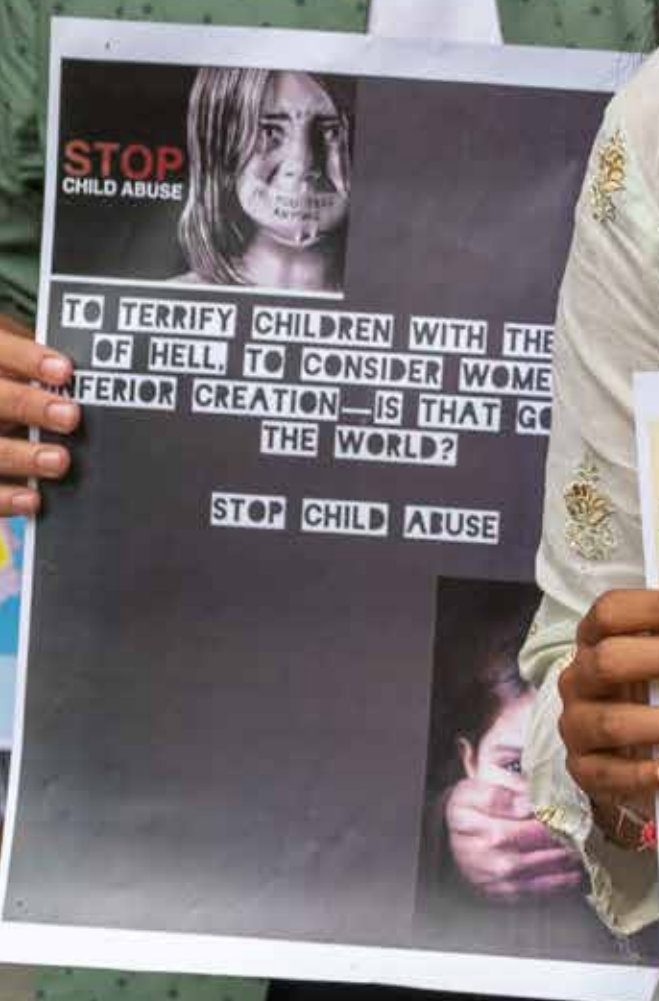
These barriers and challenges should be taken into consideration when developing the laws and procedures for receiving compensation for online sexual abuse and exploitation.

If a State is considering establishing a State compensation scheme or expanding the remit of an existing fund to respond to child victims of sexual abuse and exploitation, child-sensitive procedures should be integrated throughout the process. For example, applications from child victims should be assessed only by those who have received training on the impacts of sexual abuse on child victims, including the specificities of online abuse. Other elements could include an expedited application process for child victims, or procedures which ensure funds are distributed in a manner that is in the child's best interests.

Such schemes should also consider treating jurisdictional factors flexibly, and make funding available for child victims, even if they are not nationals residents or if the perpetrator resides in another country. This was recognized by the CRC Committee when they outlined the need to *'Guarantee that all child victims, including those who are not nationals or residents of the State party, have access to adequate procedures to seek, without discrimination, compensation from those legally responsible... and establish a victims' compensation fund for those cases where victims cannot obtain compensation from the perpetrators'*⁶⁴³

Endnotes

- 587 OPSC Guidelines, Para. 97.
- 588 ECOSOC Resolution 2005/20.
- 589 OPSC Guidelines, Para. 10.
- 590 *Ibid.*, Para. 47.
- 591 *Ibid.*, Para. 97(a).
- 592 *Ibid.*, Para. b.
- 593 *Ibid.*, Para. 97(a).
- 594 *Ibid.*, Para. 97(d).
- 595 IJM, Child Protective Prosecutions: A Strength-Based, Child-Centered Approach to Assess Prosecution Results, 2021. <https://osec.ijm.org/documents/64/IJM-child-protective-prosecutions-2021.pdf>
- 596 Law No. 13.431 (Brazil), 4 April 2017, <www.planalto.gov.br/ccivil_03/ato2015-2018/2017/lei/l13431.htm>, accessed 3 May 2022.
- 597 Please note that this is an unofficial translation.
- 598 Rosli, Najwa, et al., 'Regulating the Protection and Rehabilitation of Victims of Internet Child Pornography in Malaysia', International Journal of Academic Research Business and Social Sciences, vol. 9, no. 5, 2019, p. 459.
- 599 CRC/C/156, 10 September 2019, para. 17.
- 600 General Comment No. 25 (2021), para. 45.
- 601 ECPAT, Summary Paper on Online Child Sexual Exploitation, ECPAT International, Bangkok, 2020, p. 22.
- 602 OPSC Guidelines, para. 102.
- 603 Para. 13.
- 604 CRC General Comment No. 25 (2021) para. 45.
- 605 *Ibid.*
- 606 Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies, adopted by the Lanzarote Committee On 12 May 2017, para. 12.
- 607 *Ibid.*, para. 15.
- 608 ASEAN, 2019, p. 2, <<https://asean.org/declaration-on-the-protection-of-children-from-all-forms-of-online-exploitation-and-abuse-in-asean/>>
- 609 Individual online interview, Korea Legislation Research Institute, 31 March 2022.
- 610 For more information on effective strategies to respond to child sexual abuse and exploitation, see <https://www.unicef.org/media/89096/file/CSAE-Report-v2.pdf>.
- 611 OPSC Guidelines, para. 100(b).
- 612 Von Weiler, Julia, et al., Care and treatment of child victims of child pornographic exploitation (CPE) in Germany, Journal of Sexual Aggression, vol. 16, no. 2, 2010, p. 219.
- 613 International Justice Mission, A study on Online Sexual Exploitation of Children for Aftercare Reintegration, 2020, p. 26.
- 614 Whittle, Helen, et al., 'Victims' Voices: The Impact of Online Grooming and Sexual Abuse', Universal Journal of Psychology, vol. 1, no. 2, 2013, p. 68.
- 615 General Comment No. 25 (2021), Para. 47.
- 616 *Ibid.*, Para. 33.
- 617 ECOSOC Resolution 2005/20: Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, para. 40.
- 618 *Ibid.*, para. 42.
- 619 CRC General Comment No. 25 (2021), para. 45.
- 620 ECOSOC Resolution 2005/20: Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, Para. 43.
- 621 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, November 2016, p. 18.
- 622 CRC General Comment No. 19 (2008), para. 21(a).
- 623 OPSC Guidelines, para. 27.
- 624 CRC General Comment No. 25 (2021), para. 28.
- 625 Rackley, Erika, et al., 'Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse', Feminist Legal Studies, vol. 29, no. 3, November 2021, p. 318.
- 626 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, November 2016, p. 21.
- 627 UNICEF, Victims Are Not Virtual: Situation assessment of online child sexual exploitation in South Asia, 2021, p. 62.
- 628 Child Helpline International provides a list of helplines around the world: <https://childhelplineinternational.org/helplines/>. It also provides guidance and training on helplines for members.
- 629 UNICEF and Child Helpline International, A new reality child helplines report on online child sexual exploitation and abuse around the world, 2017, p. 25-26.
- 630 ECPAT, Summary Paper on Online Child Sexual Exploitation, ECPAT International, Bangkok, 2020, p. 20-22; INHOPE, Hotline Development Guide: Chapter 5 Practical aspects of creating a hotline, <www.inhope.org/media/pages/hotline-guide/the-issue/practical-aspects-of-creating-a-hotline/c38cbf4c29-1647828974/chapter-5-practical-aspects-of-creating-a-hotline.pdf>, 29 March 2022; UNICEF, Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York, 2021.
- 631 General Comment No. 13 (2011) on the Right of the child to freedom from all forms of violence states, para. 72(h).
- 632 Rosli, Najwa, et al., 'Regulating the Protection and Rehabilitation of Victims of Internet Child Pornography in Malaysia', International Journal of Academic Research Business and Social Sciences, vol. 9, no. 5, 2019, p. 459.
- 633 OPSC Guidelines, para. 106.
- 634 CRC General Comment No. 25 (2021), para. 46.
- 635 UNICEF, Victims Are Not Virtual: Situation assessment of online child sexual exploitation in South Asia, 2016, p. 34.
- 636 Rosli, Najwa, et al., 'Regulating the Protection and Rehabilitation of Victims of Internet Child Pornography in Malaysia', International Journal of Academic Research Business and Social Sciences, vol. 9, no. 5, 2019, p. 459.
- 637 OPSC Guidelines, para. 105. Also see: ECPAT, Barriers to Compensation for Child Victims of Sexual Exploitation A discussion paper based on a comparative legal study of selected countries, Bangkok, Thailand, May 2017, p. 33.
- 638 OPSC Guidelines, para. 106.
- 639 ECPAT, Barriers to Compensation for Child Victims of Sexual Exploitation A discussion paper based on a comparative legal study of selected countries, Bangkok, Thailand, May 2017, p. 15.
- 640 *Ibid.*, p. 17.
- 641 *Ibid.* See also, Binford, W., 'A Global Survey of Country Efforts to Ensure Compensation for Child Pornography Victims', Ohio State Journal of Criminal Law, vol. 13, no. 37, April 2015, p.27.
- 642 ECPAT, Barriers to Compensation for Child Victims of Sexual Exploitation A discussion paper based on a comparative legal study of selected countries, Bangkok, Thailand, May 2017, p. 22.
- 643 Committee on the Rights of the Child, Consideration of Reports Submitted by States Parties Under Article 12, Paragraph 1, of the Optional Protocol to the Convention of the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Concluding Observations: Sweden, U.N. Doc. CRC/C/OPSC/SWE/CO/1, 7 October 2011, para. 36(b).



10. Independent monitoring and regulation

Checklist of minimum and recommended standards

Ensure that children's rights in relation to the digital environment, including their rights to protection, are integrated into the legislative mandate and activities of the State's NHRI for children

Children's online protection **should** be integrated within the mandate of independent regulatory systems for the digital environment, which should work in collaboration with other monitoring bodies, particularly the NHRI, to protect children from online child sexual exploitation and abuse

Consider the establishment of an independent regulator for online safety, including the protection of children from online sexual exploitation and abuse

10.1 Detail of minimum and recommended standards

Ensure that children's rights in relation to the digital environment, including their rights to protection, are integrated into the legislative mandate and activities of the State's NHRI for children

Independent monitoring of children's rights in the digital environment is a critical part of protecting children from online child sexual exploitation and abuse. The primary means of independent monitoring of children's rights to protection in the digital environment is through a national human rights institution (NHRI).

The basis for establishing a NHRI to protect and promote children's rights is well-established under international standards. The Paris Principles, which were adopted by the General Assembly in resolution 48/134 of 20 December 1993, set out the standards for the status of NHRIs. Though the Paris Principles do not specifically mention children's rights, they make it clear that the monitoring of human rights is integral to the work of NHRIs in:

- **Protecting** human rights, which includes '*monitoring, inquiring, investigating and reporting on human rights violations*'; and
- **Promoting** human rights through activities such as education, public outreach and advocacy '*which seek to create a society where human rights are more broadly understood and respected*'⁶⁴⁴ (which can in turn be thought of as strengthening the demand for the monitoring of children's rights and contributing to creating a culture of accountability).

The CRC Committee makes it clear that the establishment of an independent monitoring mechanism falls squarely under a State party's general measures of implementation under Article 4 of the CRC.⁶⁴⁵ This monitoring mechanism should complement the monitoring mechanisms established within government.

In terms of institutional structure, the CRC Committee recommends that *'[a] broad-based NHRI should include within its structure either an identifiable commissioner specifically responsible for children's rights, or a specific Section or division responsible for children's rights'*.⁶⁴⁶ The rationale for this is that, when resources are limited, *'consideration must be given to ensuring that the available resources are used most effectively for the promotion and protection of everyone's human rights, including children's, and in this context development of a broad-based NHRI that includes a specific focus on children is likely to constitute the best approach'*.⁶⁴⁷

✓ Children's rights in the digital environment, including their rights to protection, should fall within the scope of the NHRI's mandate and activities, set out in the law, to protect and promote children's rights in line with these international standards.⁶⁴⁸ An NHRI's activities in relation to children's rights in the digital environment should include:

- The power to receive, investigate and address complaints from children and their representatives;
- Undertaking investigations into violations of children's rights, either in response to individual complaints or on its own initiative;
- Conducting independent inquiries on matters relating to children's rights;
- Preparing and publicizing opinions, recommendations and reports, either at the request of national authorities or on their own initiative, on matters relating to the promotion and protection of children's rights;
- Keeping under review the adequacy and effectiveness of law and practice relating to the protection of children's rights;
- Promoting harmonization of national legislation, regulations and practices with the CRC, its Optional Protocols and other international human rights instruments relevant to children's rights and promote their effective implementation, including through the provision of advice to public and private bodies in construing and applying the CRC;

- Ensuring that national economic policymakers take children's rights into account in setting and evaluating national economic and development plans;
- Ensuring that the impact of laws and policies on children is carefully considered from development to implementation and beyond;
- Reviewing and reporting on the government's implementation and monitoring of the state of children's rights, seeking to ensure that statistics are appropriately disaggregated, and other information collected on a regular basis in order to determine what must be done to realize children's rights;
- Contributing independently to the reporting process under the CRC and other relevant international instruments and monitor the integrity of government reports to international treaty bodies with respect to children's rights, including through dialogue with the CRC Committee at its pre-sessional working group and with other relevant treaty bodies.⁶⁴⁹

✓ The law should explicitly outline the scope of the NHRI's activities with regard to private entities, particularly whether the NHRI is able to act on complaints or reports of rights violations by private entities as well as State bodies.

In practice, where independent oversight bodies exist to monitor activities in relation to the digital environment (on which see further below), NHRIs should work closely with such bodies on effectively discharging their mandate regarding children's rights.⁶⁵⁰

Example: England

The work of the Children's Commissioner for England, the mandate for which is established in the Children Act 2004 and strengthened under the Children and Families Act 2014, includes a focus on the rights of children in the digital environment. Through this work, the Children's Commissioner aims to *'protect and empower children online'* as well as hold *'social media companies to account'*.⁶⁵¹ The Children's Commissioner publishes information on and raises awareness of children's rights in the digital environment, as well as the right to protection from online child sexual exploitation and abuse.⁶⁵²

Children’s online protection **should** be integrated within the mandate of independent regulatory systems for the digital environment, which should work in collaboration with other monitoring bodies, particularly the NHRI, to protect children from online child sexual exploitation and abuse

Another way in which children’s online protection can be monitored is through the role of independent regulatory systems of the digital environment. International and regional child rights instruments do not specify the way in which the independent regulation of the digital sector should be achieved. Rather, the CRC Committee recommends that States parties should ensure that the mandates of NHRIs ‘*and other appropriate independent institutions*’ (emphasis added) cover children’s rights in the digital environment, and that NHRIs should work together with independent oversight bodies of the digital environment (where such bodies exist) to monitor activities in relation to the digital environment.⁶⁵³

The CRC Committee also provides the following guidance more generally with regards to the regulation of the digital environment:

- States parties should ensure that, in all actions regarding the regulation of the digital environment, the best interests of every child is a primary consideration;⁶⁵⁴
- States parties should ensure that regulations, industry codes, design standards and action plans are implemented in accordance with national policies for children’s participation in the digital environment, with such national policies aiming to provide children with safe access to the digital environment as well as opportunities to benefit from engaging in the digital environment;⁶⁵⁵
- States parties should require all businesses that affect children’s rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services, including requiring businesses to maintain high standards of transparency and accountability and encouraging them to take

measures to innovate in the best interests of the child;⁶⁵⁶

- 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 regulatory frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment, including sexual exploitation and abuse.⁶⁵⁷

The ACRWC Committee similarly recommends that States parties adopt appropriate regulatory frameworks to hold businesses, which are found to have participated in sexual abuse and exploitation, accountable.⁶⁵⁸

Example: United Kingdom of Great Britain and Northern Ireland



The Online Safety Bill would provide Ofcom, the UK’s existing independent regulator for communications services, with responsibilities to oversee and enforce the legal requirements imposed on online service providers (see also **Part 7: Duties and responsibilities in relation to business** for more details on the proposed new regulatory regime in the UK).⁶⁵⁹

Under the proposals, Ofcom’s powers include:

- The power to compel the online service providers falling under the scope of the Bill to provide information;
- Requiring an individual from the online service provider to attend an interview;
- Powers of entry and inspection; and
- Power to issue enforcement notifications which may set out the steps required to remedy a contravention;

- The power to impose financial penalties of up to £18 million or 10 per cent of qualifying worldwide revenue, whichever is greater;
- The power to apply to the courts in certain cases for an order to impose business disruption measures on a provider which fails to comply;
- The requirement to produce codes of conduct for online service providers setting out the recommended steps that the providers can take in order to comply with legal requirements.⁶⁶⁰

Powers include investigation and enforcement powers in relation to child sexual abuse material.

In December 2021, the Joint Committee on the Online Safety Bill noted that investigations into child sexual exploitation and abuse material fell outside of Ofcom's normal duties and therefore expected Ofcom to work closely with *'experts like the Internet Watch Foundation, to develop and update the child sexual exploitation and abuse Code of Practice; monitor providers to ensure compliance with the child sexual exploitation and abuse code; and during investigations relating to child sexual exploitation and abuse content'*.⁶⁶¹

Consider the establishment of an independent regulator for online safety, including the protection of children from online sexual exploitation and abuse

States may alternatively consider establishing an independent regulator focusing specifically on issues relating to safety in the digital environment. Mandates and powers of regulators vary depending on what is contained in the constituent legislation (See **Part 7: Duties and responsibilities in relation to business** for more details on the eSafety Commissioner in Australia as an example).

Endnotes

644 General Observations of the Sub-Committee on Accreditation of the Global Alliance of National Human Rights Institutions (GANHRI), adopted by the GANHRI Bureau at its meeting in Geneva on 21 February 2018, p. 7.

645 Committee on the Rights of the Child, General Comment No. 5 (2003) on General measures of implementation of the Convention on the Rights of the Child, CRC/GC/2003/5, 27 November 2003, para. 27.

646 Committee on the Rights of the Child, General Comment No. 2 (2002) on the role of independent national human rights institutions in the promotion and protection of the rights of the child, CRC/GC/2002/2, 15 November 2002 (CRC Committee GC No. 2 (2002)), para. 6.

647 CRC Committee General Comment No. 2 (2002), para. 6.

648 CRC General Comment No. 25 (2021), para. 31.

649 CRC Committee in General Comment No. 2, para. 20; CRC General Comment No. 25 (2021), para. 31.

650 CRC General Comment No. 25 (2021), para. 31.

651 Children's Commissioner for England, 'Digital' page on the website of the Commissioner, <www.childrenscommissioner.gov.uk/digital/>, accessed 18 February 2022.

652 Ibid.

653 CRC General Comment No. 25 (2021), para. 31.

654 Ibid.

655 Ibid., para. 24.

656 Ibid., para. 39.

657 Ibid., para. 82.

658 ACRWC GC 7, para. 138.

659 Online Safety Bill (UK) published 17 March 2022, Part 7, <https://bills.parliament.uk/bills/3137>, accessed 24 May 2022.

660 Explanatory Notes to the Online Safety Bill (drafted dated 17 March 2022), Bill 285-EN, pp. 9-11.

661 Joint Committee on the Draft Online Safety Bill, Parliament of the United Kingdom, Report of Session 2021-22 - published 14 December 2021 - HL Paper 129 - HC 609, Conclusions and Recommendations, para. 83, <https://publications.parliament.uk/pa/it5802/jtselect/jtonline-safety/129/12902.htm>, accessed 24 May 2022.



11. Implementation of legislation

Checklist of minimum and recommended standards

Secondary legislation, including Standard Operating Procedures and Guidelines, and other authoritative guidance to give effect to primary legislation **should** be developed to combat online child sexual abuse and exploitation

Ensure children are educated on their rights and responsibilities in the digital environment, including on the risks of online sexual exploitation and abuse, safe online practices and available support and reporting mechanisms

Ensure parents and caregivers are educated on the digital environment, including its benefits, the risks of online sexual exploitation and abuse, safe online practices and available support and reporting mechanisms

Professionals who work with and for children **should** receive training on the identification of children at risk, support services and reporting mechanisms, and opportunities and risks in relation to the digital environment, including different forms of technology

Law enforcement professionals **should** receive training in best practice that is contextualized to the countries' legal framework for the effective investigation and prosecution of online offences

Ensure sufficient financial and human resources are allocated annually to give effect to legislation designed to combat online child sexual abuse and exploitation

States parties **should** develop secondary legislation, including Standard Operating Procedures and Guidelines, to give effect to primary legislation developed to combat online child sexual abuse and exploitation

11.1 Detail of minimum and recommended standards

Secondary legislation, including Standard Operating Procedures and Guidelines, and other authoritative guidance to give effect to primary legislation **should** be developed to combat online child sexual abuse and exploitation

International standards

In order to ensure the smooth implementation of legislation to combat online child sexual abuse and exploitation the CRC Committee's General Comment No. 25 (2021) recommends that States parties should *'ensure that national policies relating to children's rights specifically address the digital environment'* to protect children's online safety.⁶⁶² This includes the creation of secondary legislation

and other authoritative guidance which give effect to primary legislation.

Alongside this, the CRC Committee recommends that children's online protection should be integrated into existing child protection policies and practices to ensure children are protected from online risks to the same extent as they are safeguarded from harm offline.⁶⁶³ States parties should also *'implement measures'* to ensure the efficient investigation of online child sexual exploitation and abuse.⁶⁶⁴

Regional standards

Regional instruments also reinforce the importance of ensuring primary legislation is given effect in secondary legislation. The Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN, for instance, provides Member States with guidance on how to implement the ASEAN Declaration and strengthen their own national legal and policy frameworks.

In a similar vein to the ASEAN Regional Plan of Action, the Council of Europe introduced the *'Handbook for Policy Makers on the Rights of the Child in the Digital Environment'*⁶⁶⁵ in 2020 to support the implementation of their *'Guidelines to respect, protect and fulfil the rights of the child in the digital environment'*.⁶⁶⁶ This Handbook advises States on how to implement the Guidelines, as well as provides concrete action points on how states could engage and work in conjunction with relevant stakeholders.⁶⁶⁷

Example: Ghana

Since the passing of the Cybersecurity Act (2020) in Ghana, which introduces a range of online sexual exploitation and abuse offences, UNICEF has been working with the Ministry of Communications to introduce sentencing guidelines on crimes set out in the law, adopting a similar approach to that taken in the United Kingdom. In anticipation of new legislation, starting in 2019, UNICEF has been working alongside the Internet Watch Foundation and the Ministry of Communications to develop an online portal for reporting online child sexual exploitation and abuse content. The portal was launched in October 2020 and seeks to complement the existing Point of Contact referral mechanism to *'provide a safe platform for people to report suspected child sexual abuse materials'*.⁶⁶⁸ This collaboration has helped to develop the referral pathway for suspected child sexual abuse material in Ghana, and has given effect to the new Cybersecurity Act.

In addition, UNICEF is currently working with telecommunication companies with operations in Ghana to advance notice and takedown procedures related to online child sexual abuse and exploitation, building the capacity of industry partners to combat online child sexual abuse and exploitation taking place via their platforms.⁶⁶⁹

- ✓ States should consider building in provisions for the development of secondary legislation into newly created laws. Given the pace at which technology evolves, secondary legislation is particularly important as it allows decision makers to ensure that legislative protections for children keep pace with new forms of digital harm.

Example: Australia



Australia has dealt with this challenge by giving the eSafety Commissioner the power to provide guidance and set expectations for industry, so that they can address new and emerging issues in a timely and flexible manner without needing to amend or pass new primary legislation.⁶⁷⁰

The Australian Online Safety Act (2021) provides that one of the roles of the eSafety Commissioner, as set out in Article 27 (1)(p) of the Act is:

'(p) to formulate, in writing, guidelines or statements that:

- (i) recommend best practices for persons and bodies involved in online safety for Australians; and
- (ii) are directed towards facilitating the timely and appropriate resolution of incidents involving material provided on a social media service, relevant electronic service or designated Internet service; and

(q) to promote guidelines and statements formulated under paragraph (p); and (r) such other functions'.⁶⁷¹

✓ States should consider creating a coherent framework of secondary legislation and other authoritative guidance, including guidelines, policies and codes to give effect to the primary legislation. Such instruments should be reviewed regularly to ensure there are no gaps or unintended consequences. More information on this can be found in **Part 5: Methods of legislative reform**. Where gaps exist in terms of implementation and place children at risk of online child sexual exploitation and abuse, States should initiate and/

or amend secondary legislation. All guidelines must be in line with international human rights standards, particularly General Comment No. 25 (2021) of the CRC.

States should ensure that all legislation is cross-sectoral given the nature of online sexual abuse and exploitation. Clear guidelines on referral mechanisms need to be made available to all mandatory reporting bodies, including healthcare professionals, teachers and social workers.

Ensure children are educated on their rights and responsibilities in the digital environment, including on the risks of online sexual exploitation and abuse, safe online practices and available support and reporting mechanisms

Ensure parents and caregivers are educated on the digital environment, including its benefits, the risks of online sexual exploitation and abuse, safe online practices and available support and reporting mechanisms

International standards

Ensuring children and their parents/caregivers are informed on children's rights in the digital environment, together with the risks of online sexual exploitation and abuse and avenues for redress is essential to prevent and respond to online child sexual abuse and exploitation. Article 19 of the CRC calls on states to use all appropriate measures to prevent violence against children, including 'social and educational measures'.⁶⁷² The Committee's General Comment No. 25 (2021) elaborates this requirement: States should 'disseminate information and conduct awareness-raising campaigns on the rights of the child in the digital environment, focusing in particular on those whose actions have a direct or indirect impact on children'.⁶⁷³ This includes the development of educational programming for children and families, members of the public and decision-makers, which includes information on the benefits and harms of digital products and services.

✓ The CRC Committee specifically recommends that children and families should be empowered through the development of children's digital

literacy, including information on how to protect their privacy, prevent victimization, and recognize and respond to a child at risk of harm in the digital environment.⁶⁷⁴

✓ In order to ensure children are fully aware of their rights and able to access reporting and complaint mechanisms, services and support, educational content should be provided to children in an age-appropriate manner, using child-friendly language.⁶⁷⁵

Regional standards

In most regional standards there is an acknowledgement of the important role education of children, parents, caregivers and the general public plays in preventing and responding to online child sexual exploitation and abuse. In particular:

- The ASEAN Declaration outlines the need for Member States to promote 'a national education programme and school curricula to raise awareness of sexual, and other forms of exploitation of children to empower children, young people, parents, guardians, caregivers, practitioners and community'.⁶⁷⁶

- The Lanzarote Convention includes recommendations that States parties should *'prevent CSEA, including through recruitment, training and awareness-raising of persons working in contact with children, educating children about the risks of CSEA and how to protect themselves'*.⁶⁷⁷
- The 2016 Guidelines for the Adoption of National Legislation in Latin America recommends that countries have *'specific public policies for prevention, awareness, and comprehensive care'* for victims of online sexual abuse.⁶⁷⁸

Professionals who work with and for children **should** receive training on the identification of children at risk, support services and reporting mechanisms, and opportunities and risks in relation to the digital environment, including different forms of technology

Law enforcement professionals **should** receive training in best practice that is contextualized to the countries' legal framework for the effective investigation and prosecution of online offences

International standards

In order to protect children, professionals who work with them should be equipped with the knowledge and skills to identify and report online child sexual abuse and exploitation.⁶⁷⁹ The CRC Committee Guidelines on the Implementation of the OPSC sees the provision of education and continued training of all relevant professionals as an integral part of any national policy and strategy for the implementation of the OPSC.⁶⁸⁰ The Guidelines also recommends that States parties train all police units investigating offences covered by the OPSC, *'including when these offences are facilitated or committed through ICT, as well as prosecutors and the judiciary, to identify and respond to child victims in a child- and gender-sensitive manner and to handle cases associated with ICT and digital evidence'*.⁶⁸¹

The CRC Committee in General Comment No. 25 also pays particular attention to the need to train law enforcement and justice personnel and recommends that *'States provide specialized training for law enforcement officials, prosecutors and judges regarding child rights violations specifically associated with the digital environment'*⁶⁸² and that *'specialized training for law enforcement officials, lawyers, prosecution and judiciary professionals should include specific*

components on online issues, but also on online tools to facilitate victim identification techniques and rescue operations'.⁶⁸³

Legislation should contain a requirement for regular training for law enforcement and justice professionals and ensure protected time to allow them to attend such training. Training should take place at the national and local level, with ongoing refresher training to ensure that professionals are kept up to date with new legislation, guidance and best practice.⁶⁸⁴ Training needs to be contextualized to the national and local context to ensure it is relevant and effective.

Other professionals, and especially educational professionals, working *'for and with children'* should also receive training on the impact of the digital environment on children and their use of digital technologies.⁶⁸⁵

The CRC Committee further recommends that industry professionals in the business and technology sectors should be trained on the impact of the digital environment on children, and the application of international human rights law to the digital environment.⁶⁸⁶ Additionally, digital service providers should be trained on the identification of children who are at risk of harm.⁶⁸⁷

Regional standards

Regional instruments affirm the need for training of professionals on tackling child sexual exploitation and abuse in the digital environment. Article 35.3 Budapest Convention provides that *'[e]ach Party shall ensure that trained and equipped personnel are available'*, in order to facilitate the operation of the 24-hour, 7-day-a-week network.

The African Committee General Comment No. 7 of the ACRWC (2021) notes that there are few African States that have cybercrime law enforcement units. At the same time it recognises that tackling the new and emerging forms of child online sexual exploitation requires dedicated and well-trained staff with modern era skills and competencies and requires law enforcement, such as police and prosecutors, to be specialized in computer and digital media analysis in order to collect evidence.⁶⁸⁸

The ASEAN Declaration highlights as a priority the need to enhance *'law enforcement, judicial and legal professional capabilities through regular, relevant and updated trainings and sharing and exchange of best practices in the protection of children against all forms of online exploitation and abuse'*. One of the aims of the ASEAN Working Group on Cybercrime is to develop capability

building and training initiatives, with the Group's TOR outlining how they *'will develop regional training programmes and regular conferences to enhance capabilities in combating cybercrime'*.⁶⁸⁹ Additionally, the 2016 Guidelines for the Adoption of National Legislation in Latin America recommend that *'a plan for continuous training and professional development should be developed for undercover agents, as well as for those who authorize their activities'*.⁶⁹⁰

✓ Some countries provide their law enforcement personnel with specialized courses in online child sexual exploitation, including digital technology and software and child forensic interviews. Where this is not provided, States should consider approaching INTERPOL, CEPOL (for EU Member States) and the European Cybercrime Training and Education Group, which all offer training, as do a number of private providers. Study visits or hosting foreign law enforcement delegates to exchange good practices are another valuable way of providing law enforcement with the necessary skills. Consideration should be given as to how all training can be tailored to ensure it is highly contextualized and developed with country-specific legal frameworks,⁶⁹¹ social and cultural practices in mind.

Ensure sufficient financial resources are allocated annually to give effect to legislation designed to combat online child sexual abuse and exploitation

Without sufficient recurring funds in annual budgets, the ability of States to implement legislation on online child sexual abuse and exploitation would be severely limited. Article 4 of the UN Convention on the Rights of the Child requires that *'States parties [...] undertake all appropriate legislative, administrative and other measures for the implementation of the rights recognized in the Convention'*.⁶⁹² In interpreting this Article of the CRC General Comment No. 19 (2016) recommends that States should ensure sufficient financial resources are made available to ensure children's rights are realized. In order to implement this, States parties should ensure that:

'(a) Laws and policies are in place to support resource mobilization, budget allocation and spending to realize children's rights;

(b) The necessary data and information about children are collected, generated and disseminated to support the design and implementation of appropriate legislation, policies, programmes and budgets to advance the rights of the child;

(c) Sufficient public resources are mobilized, allocated and utilized effectively to fully

implement approved legislation, policies, programmes and budgets;

(d) Budgets are systematically planned, enacted, implemented and accounted for at the national and subnational levels of the State, in a manner that ensures the realization of children's rights.⁶⁹³

Specific mention of allocating funds to prevent online child sexual exploitation and abuse is contained in General Comment No. 25 (2021) which recommends that 'States parties should mobilize, allocate and utilize public resources to implement legislation, policies and programmes to fully realize children's rights in the digital environment'.⁶⁹⁴ Additionally, General Comment No. 13 (2011) states that States parties should provide budget allocations '*for the implementation of legislation and all other measures adopted to end violence against children*'⁶⁹⁵ and to provide '*adequate protection of children in relation to media and ICT*'.⁶⁹⁶

Ensuring sufficient human and financial resources are available to implement proposed legislation fully is vital to ensuring the implementation of laws to combat online child sexual exploitation and abuse.

As well as funds required to deal with the increased number of cases being dealt with by the child protection and justice systems arising from online child sexual exploitation and abuse, funding is also required to:

- Upscale current data collection efforts to include crimes related to online child sexual abuse and exploitation;
 - Conduct research and monitor the implementation of any legislation;
 - Submit and respond to other States requests under the Mutual Legal Assistance Procedure;
 - Deliver regular training of professionals who work with children, including referrers (i.e. teachers, medical staff, youth workers), social workers, justice professionals and law enforcement staff to equip them with the knowledge and skills to respond to online child sexual abuse and exploitation cases;
 - Provide specialized services and support for victims of online child sexual abuse and exploitation; and
 - Provide contextualized counselling and psychological care for professionals who are at risk of experiencing secondary traumatic stress or vicarious trauma due to exposure to CSAM or related harmful content.⁶⁹⁷
- ✓ '*It's one thing to have a law, and another thing to have the law implemented*'.⁶⁹⁸ States should ensure annual budget processes take into consideration the additional resource implications of any new legislation that is developed.
- Provide adequate office space, office furniture, strong internet, secure computers, and other necessary basic law enforcement infrastructure;
 - Deliver prevention programming, awareness and educational activities related to online safety;
 - Adequately prevent, respond to and investigate digital crimes, including the purchasing of specialized ICT equipment by law enforcement;
 - Develop digital forensics capabilities;
 - Adequately staff and provide resources for a regulatory body;
 - Provide training for the business and technology sectors on the identification and referral of children at risk of harm;

Endnotes

- 662 CRC General Comment No. 25 (2021), para. 24.
- 663 Ibid., para. 25.
- 664 Ibid.
- 665 Council of Europe, Handbook for Policy Makers on the Rights of the Child in the Digital Environment, <<https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>>, accessed 28 May 2022.
- 666 Council of Europe, Recommendation CM/Rec(2018)7, <<https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>>
- 667 Livingstone, Sonia, et al, Handbook for Policy Makers on the Rights of the Child in the Digital Environment. Council of Europe, p. 11, <www.coe.int/en/web/children/-/all-on-board-all-online-launch-of-the-new-council-of-europe-handbook-for-policy-makers-on-the-rights-of-the-child-in-the-digital-environment?inheritRedirect=true>, accessed 2 March 2022.
- 668 Appiah, N, Communication Ministry and IWF launch Ghana's Child Online Protection Reporting Portal, BizTech Africa, 2 October 2020. www.biztechafrika.com/article/communication-ministry-and-iwf-launch-ghanas-child/16146/, accessed 28 May 2022.
- 669 End Violence Against Children, In Ghana, a Law to Address Online Child Sexual Exploitation is Approved, 18 June 2021, www.end-violence.org/articles/ghana-law-address-online-child-sexual-exploitation-approved, accessed 2nd March 2022.
- 670 Online individual interview, Office of the eSafety Commissioner of Australia, 22 March 2022.
- 671 Online Safety Act 2021 (Australia), Article 27 (1)(p).
- 672 UNCRC (1991), Article 19.
- 673 CRC General Comment No. 25 (2021), para. 32.
- 674 Ibid.
- 675 CRC General Comment No. 25 (2021), para. 49.
- 676 Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, paras. A-G.
- 677 Lanzarote Convention, Chapter 2.
- 678 UNICEF Latin America and Caribbean Regional Office and ICMEC, Online Child Sexual Abuse and Exploitation, Guidelines for the Adoption of National Legislation in Latin America, 2016, p. 18.
- 679 OPSC Guidelines, para. 30.
- 680 Ibid.
- 681 Ibid., para. 30(c).
- 682 CRC General Comment No. 25 (2021), para. 47.
- 683 OPSC Guidelines para. 39.
- 684 IACAT, IJM, US Department of States Office to Monitor and Combat trafficking in Persons, 2020, Online Sexual Exploitation of Children in the Philippines, <https://www.ijm.org/vawc/blog/osec-study>, accessed 24 May 2022; UNICEF, Child Protection in the Digital Age, 2016, <www.unicef.org/eap/reports/child-protection-digital-age>, and Speller E., Protection against Child Sexual Exploitation and Abuse in the Commonwealth: Research Mapping Report (undated), <<https://itsapenalty.org/wp-content/uploads/2020/03/ET-CSEA-Legislation-in-Commonwealth-Research-Mapping-Report.pdf>>
- 685 CRC General Comment No. 25 (2021), para. 33.
- 686 Ibid.
- 687 Ibid., para. 45.
- 688 ACRWC General Comment No. 7, para. 107.
- 689 ASEAN working Group on Cyber Crime, Terms of Reference. Adopted at the Inaugural SOMTC Working Group on Cybercrime Singapore, 27 May 2014.
- 690 UNICEF Latin America and Caribbean Regional Office and ICMEC, Online Child Sexual Abuse and Exploitation, Guidelines for the Adoption of National Legislation in Latin America, 2016, p. 18.
- 691 Including both primary and secondary legislation.
- 692 UNCRC (1991), Article 4.
- 693 CRC General Comment No. 19 (2016), para. 21.
- 694 CRC General Comment No. 25 (2021), para. 28.
- 695 CRC General Comment No. 13 (2011), para. 41e.
- 696 Ibid., para. 41g.
- 697 UNICEF, Ending Online Child Sexual Exploitation and Abuse: Lessons Learned and promising practices in low and middle income countries, UNICEF, New York, December 2021, p. 2, <https://www.unicef.org/documents/ending-online-child-sexual-exploitation-and-abuse> p.36.
- 698 Online individual interview, Justice for Children Zimbabwe, 29 March 2022.



12. Glossary

Artificial Intelligence (AI)	The simulation of human intelligence in machines, through replicating traits associated with a human mind, such as learning and problem-solving. Machine learning, a subset of AI, refers to when computer programs automatically learn from and adapt to new data without human assistance. Deep learning techniques facilitate automatic learning through the absorption of data such as text, images or video. ⁶⁹⁹
Bandwidth	A measure concerning <i>‘the amount of data that can be transferred from one point to another within a network in a specific amount of time. Typically, bandwidth is expressed as a bitrate and measured in bits per second (bps)’</i> . Bandwidth is vital factor in determining the quality and speed of a network. ⁷⁰⁰
Bitcoin	A digital currency which operates free of any central control (i.e. the oversight of banks or governments), and instead relies on peer-to-peer software and cryptography. ⁷⁰¹
Caching / Cashing	The process of storing data in either a hardware or software cache, so that future requests for that data can be served faster. ⁷⁰²
Child Rights Impact Assessment (CRIA)	Tool for predicting the impact of any proposed law, policy or budgetary allocation, which affects children and the enjoyment of their rights. ⁷⁰³
Content	All multi-media content found on online platforms, such as text, images, audio and video files etc.
Content rights	The ownership rights, i.e. copyright or other Intellectual Property rights, to content. ⁷⁰⁴
Cyberbullying	Bullying (i.e. repeated behaviour aimed at scaring, angering or shaming) a person with the use of digital technologies. ⁷⁰⁵
Cyberflashing	The unsolicited sending of images (including video) of genitals with the use of digital technologies.
Cybersecurity	Protecting against the criminal or unauthorized use of electronic data, or from other cyber related attacks.
Dark Net / Dark Web	<i>‘[E]ncrypted online content that is not indexed by conventional search engines’</i> and can only be accessed using specific browsers. ⁷⁰⁶
Data controller	A legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it. ⁷⁰⁷
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller. ⁷⁰⁸
Data retention	The storing of data for a specific period of time. Data retained can be non-content data (for example, IP address, date, duration etc.) or content data (for example, the text of users’ emails or messages, images or videos).

Digital environment	Information and communications technologies, including <i>‘digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology’</i> . ⁷⁰⁹
Digital technologies	See <i>‘ICTs’</i> .
E-commerce	The buying and selling of goods and services or the transmitting of funds or data over the internet. ⁷¹⁰
Encryption	A mechanism which <i>‘scrambles communication so that it cannot be read by anyone unless they have the corresponding key to decrypt the data’</i> . ⁷¹¹
End-to-end encryption	A <i>‘particularly robust form of encryption where third party intermediaries (such as a service provider) do not have keys to decrypt the communication; it is only readable by the two parties exchanging information’</i> . ⁷¹²
Extraterritorial jurisdiction	Jurisdiction exercised outside of the territorial boundaries of a State, which is normally only exercised if there is a specific permissive rule establishing a link to the asserting State. ⁷¹³
Hash	A unique digital signature of an image.
Helplines	Helplines provide confidential advice and assistance to callers, often acting as points of referral to other service providers.
Hosting	A <i>‘service through which storage and computing resources are provided to an individual or organization for the accommodation and maintenance of a website or related services’</i> . ⁷¹⁴
Hotline	A telephone line that is able to provide immediate assistance, typically used for emergency interventions. In the context of the online sexual abuse of a child, this could entail contacting the police or securing the removal of a harmful content from a digital platform.
Hyperlinks	The <i>‘characteristic or property of an element’</i> such as a <i>‘symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed’</i> . ⁷¹⁵
ICT ecosystem	Policies, strategies, processes, information, technologies, applications and stakeholders that together make up a technology environment for a country, government or an enterprise. ⁷¹⁶
Immersive technology/ technologies	Technologies which <i>‘create distinct experiences by merging the physical world with a digital or simulated reality. Augmented reality...and virtual reality... are two principal types of immersive technologies. These technologies share many of the same qualities. However, [augmented reality]...blends computer-generated information onto the user’s real environment, while [virtual reality]... uses computer-generated information to provide a full sense of immersion’</i> . ⁷¹⁷

Information and communication technology (ICT) / digital technologies	A 'diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.)'. ⁷¹⁸
Internet protocol (IP) address	A 'unique address that identifies a device on the internet or a local network'. ⁷¹⁹
Internet service provider (ISP)	An organization that provides services for accessing and using the internet. ISPs may also provide other services such as email services, domain registration, web hosting, browser services and software packages. ⁷²⁰
Live streaming	The transmission of a live video or audio coverage using digital technologies.
Local area network (LAN)	A 'collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be any size, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school'. ⁷²¹
Made for digital	Content that is primarily produced for distribution via the internet, from 'amateur user-generated content' to 'professionally produced content'. ⁷²²
Metaverse	A 'virtual reality world characterized by a three-dimensional, multi-sensory experience (as compared to the current two-dimensional internet – text and images on flat screens)'. ⁷²³
Mutual legal assistance (MLA)	The 'process by which States seek for and provide assistance to other States in servicing of judicial document[s] and gathering evidence for use in criminal cases'. ⁷²⁴
Notice and takedown (NTD)	A 'company's procedures for receiving reports that may come from customers, employees, law enforcement or hotlines that child sexual abuse material has been discovered on the company's networks or services, and for preventing further access and distribution'. ⁷²⁵
Online services	A 'diverse segment covering the range of consumer and business services provided over the internet through browsers or application platforms. It encompasses much of what most consumers probably perceive to be the actual 'internet''. ⁷²⁶
Personal Data	Any information relating to an identified natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. ⁷²⁷
Premium rights	Professionally produced video, audio, print and gaming content that is distributed via the internet (and indeed non-internet channels such as terrestrial TV), and is paid for in a number of ways, including user subscriptions or advertising-funded broadcasters. ⁷²⁸

Processing (of personal data)	Any 'operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'. ⁷²⁹
Privacy-by-design	An approach that requires 'privacy to be incorporated into networked data systems and technologies, by default'. ⁷³⁰
Private networks	Any network where access is restricted such as a corporate network or a network in a school.
Reporting portal	A customized webpage where people can report suspected child sexual abuse material. ⁷³¹
Safety-by-design	'The practice of designing online services with the aim of ensuring users' safety as much as possible, e.g. by default safe settings for accounts of underage users or by preventing adults from contacting underage users'. ⁷³²
Sexting	Self-generated sexual content sent via mobile phone text messaging or other online messaging to others. ⁷³³
Traffic data	Data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type, of the underlying service. ⁷³⁴
Trusted flaggers	Individuals, government agencies or NGOs which have particular expertise and responsibilities for tackling illegal content online.
Uniform resource locator (URL)	A 'unique identifier' or address where a particular page or resource can be found on the internet. ⁷³⁵
User interface	The 'point of human-computer interaction and communication in a device'. This includes display screens, keyboards, a mouse, the appearance of a desktop, as well as the way a user interacts with an application or a website. ⁷³⁶
Virtual reality	A type of immersive technology which uses computer-generated information to provide a full sense of immersion. ⁷³⁷
Webcam	A 'digital camera' that is 'connected to a computer to stream live video in real time'. A webcam is usually connected by a cable to a computer or built into computer hardware. ⁷³⁸
Webhosting	A 'service that allows organizations and individuals to post a website or web page onto the internet.' A webhost, or webhosting service provider, 'is a business that provides the technologies and services needed for the website or webpage to be viewed in the internet'. ⁷³⁹

Endnotes

- 699 Investopedia, Artificial Intelligence, <www.investopedia.com/terms/a/artificial-intelligence-ai.asp>, accessed 27 April 2022.
- 700 Paessler The Monitoring Experts, IT Explained: Bandwidth, www.paessler.com/it-explained/bandwidth, accessed 24 May 2022.
- 701 New Scientist, What is bitcoin and how does it work?, <www.newscientist.com/definition/bitcoin/>, accessed 5 April 2022.
- 702 Techtarger, Caching, <<https://www.techtarget.com/searchstorage/definition/cache>>, accessed 5 April 2022.
- 703 European Network of Ombudspersons for Children, Child Rights Impact Assessment- CRIA, <https://enoc.eu/?page_id=3718>, accessed 5 April 2022.
- 704 GSMA, The Internet Value Chain: A study on the economics of the internet, May 2016, p. 14, <www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf>, accessed 1 December 2021.
- 705 UNICEF, Cyberbullying: What is it and how to stop it, <www.unicef.org/end-violence/how-to-stop-cyberbullying>, accessed 4 May 2022.
- 706 Investopedia, Dark Web, <www.investopedia.com/terms/d/dark-web.asp>, accessed 5 April 2022.
- 707 Based on the definition used in GDPR, Article 4(7).
- 708 Ibid., Article 4(8).
- 709 CRC General Comment No. 25 (2021), para. 2.
- 710 Techtarger, E-commerce, <www.techtarget.com/searchcio/definition/e-commerce>, accessed 5 April 2022.
- 711 Kardefelt-Winther, Daniel, et al., Encryption, Privacy and Children's Right to Protection from Harm, UNICEF Office of Research – Innocenti Working Paper, October 2020, p. 6, www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html, accessed 24 May 2022.
- 712 Ibid.
- 713 Witting, S., 'Transnational by Default: Online Child Sexual Abuse Respects No Borders', International Journal of Children's Rights, vol. 29, no. 3, (2021), pp. 731-764, p. 735.
- 714 Techopedia, Hosting, <<https://www.techopedia.com/definition/29023/web-hosting#:~:text=Hosting%2C%20in%20its%20most%20generic,more%20websites%20and%20related%20services>>, accessed 4 May 2022.
- 715 Southern African Development Community Model Law, Section 3(14), <www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf>, accessed 16 February 2022.
- 716 Choudrie J., Islam M., Wahid F., Bass J., Priyatma J., Information and Communication Technologies for Development, Springer, 1st ed., 2017, p. 95.
- 717 Vista Equity Partners, An Introduction to Immersive Technologies, www.vistaequitypartners.com/insights/an-introduction-to-immersive-technologies/, accessed 24 May 2022.
- 718 United Nations Educational, Scientific and Cultural Organization, Institute for Statistics, Information and Communications Technologies (ICT), <www.uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict>, accessed 17 February 2022.
- 719 Kaspersky, What is an IP Address? Definition and Explanation, <www.kaspersky.com/resource-center/definitions/what-is-an-ip-address>, accessed 5 April 2022.
- 720 Twin, Alexandra, Internet Service Provider, Investopedia, 12 August 2021, <www.investopedia.com/terms/i/isp.asp>, accessed 14 September 2021.
- 721 CISCO, What is a LAN?, <www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html>, accessed 5 April 2022.
- 722 GSMA, The Internet Value Chain: A study on the economics of the internet, May 2016, <www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf>, accessed 1 December 2021, p. 14.
- 723 Li, C and Lalani, F. How to address digital safety in the metaverse, World Economic Forum, 14 January 2022, <https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/>, accessed 13 May 2022.
- 724 UNODC, University Module Services, Module 11: International Cooperation to Combat Transnational Organized Crime, Mutual Legal Assistance, <www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html>, accessed 9 December 2021.
- 725 GSMA and UNICEF, Notice and Takedown: Company policies and practices to remove online child sexual abuse material, May 2016, p. 5.
- 726 GSMA, The Internet Value Chain: A study on the economics of the internet, May 2016, <www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf>, accessed 1 December 2021, p. 15.
- 727 GDPR, Article 4(1).
- 728 GSMA, The Internet Value Chain: A study on the economics of the internet, May 2016, <www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf>, accessed 1 December 2021, p. 14.
- 729 GDPR, Articles 4(1) and 94.
- 730 Cavoukian, Ann, Privacy by Design: The 7 Foundational Principles, Information and Privacy Commissioner, Ontario, Canada, <www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>, accessed 31 March 2022.
- 731 IWF Reporting Portals, <www.iwf.org.uk/about-us/our-international-work/reporting-portals/>, accessed 1 April 2022.
- 732 CRC Committee, General Comment No. 25 (2021) Children's rights in relation to the digital environment Glossary, 12 February 2021.
- 733 OPSC Guidelines, para. 42.
- 734 Budapest Convention, Article 1(d).
- 735 Techtarger, URL, <www.techtarget.com/searchnetworking/definition/URL>, accessed 5 April 2022.
- 736 Techtarger, User Interface, <www.techtarget.com/searchapparchitecture/definition/user-interface-UI>, accessed 5 April 2022.
- 737 Vista Equity Partners, An Introduction to Immersive Technologies, www.vistaequitypartners.com/insights/an-introduction-to-immersive-technologies/, accessed 24 May 2022.
- 738 Lifewire, What is a webcam?, <www.lifewire.com/what-is-a-webcam-4844083>, accessed 7 April 2022.
- 739 Website.com, Web Hosting, <www.website.com/beginnerguide/web-hosting/6/1/what-is-web-hosting?.ws>, accessed 7 April 2022.

