



ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION

Current forms and good practice
for prevention and protection

Nikoleta Lydaki Simantiri
June 2017

This report was written by Nikoleta Lydaki Simantiri, in collaboration with ECPAT France and ECPAT Luxembourg.

Published in June 2017

Copyright ECPAT France and ECPAT Luxembourg

Design by Ophélie Rigault

Photographies by Javier Santamaría and Ophélie Rigault

The information and views set out in this publication are those of the author and do not necessarily reflect the official opinion of the French Agency for Development (AFD) or the Luxembourg Ministry for Foreign and European Affairs.



FOREWORD

ECPAT is an expanding network of local civil society organisations and coalitions that share one common goal: to end the sexual exploitation of children around the world.

ECPAT conducts research to build the collective understanding of child sexual exploitation. Together with our members and partners, we coordinate evidence-based advocacy at all levels to strengthen national justice and protection systems and to increase investment in combating the sexual exploitation of children.

In line with ECPAT International's mission, **ECPAT France** and **ECPAT Luxembourg** aim to realise the right of all children to live free from all forms of sexual exploitation.

This study has been commissioned as part of the programme “REPERES”¹ led by ECPAT France and ECPAT Luxembourg which aims at strengthening the protection of children against sexual abuse and exploitation in 14 countries of Africa and the MENA region² by sharing tools, experience and best practice between partners. REPERES is a 3-year project, co-financed by the AFD (Agence Française de Développement) and the Ministry of Foreign and European Affairs of the Grand Duchy of Luxembourg.

The present report specifically addresses the issue of online child sexual abuse and exploitation, identifying and proposing good practice with a view to raising awareness. This report does not examine the current level of national response in the 14 countries targeted by the REPERES programme nor does it identify inadequacies. Rather, it aims to provide guidance enabling these countries to detect possible shortcomings and take necessary action.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to the following persons who shared their knowledge and expertise in order to make this report possible:

Nicolas D’Arcy and Quentin Aoustin, permanent team of the French Internet Service Providers Association (AFPI)

Arda Gerkens, INHOPE President and Managing Director of the Dutch Hotline

Marie-Laure Lemineur, Head of Programme Combating Sexual Exploitation of Children Online, ECPAT International

Gioia Scappucci, Executive Secretary to the Lanzarote Committee, Council of Europe

TABLE OF CONTENTS

ACRONYMS.....	2
INTRODUCTION.....	3
SECTION 1: DEFINING ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION.....	5
1. Childhood and the age of sexual consent.....	6
2. Child sexual abuse and child sexual exploitation.....	7
3. Online child sexual abuse and online child sexual exploitation.....	8
4. Child sexual abuse material and child sexual exploitation material.....	10
5. Live online child sexual abuse.....	14
6. Solicitation of children for sexual purposes.....	15
SECTION 2: GOOD PRACTICE FOR PROTECTING CHILDREN AGAINST ONLINE SEXUAL ABUSE AND EXPLOITATION.....	19
1. National action plan.....	20
2. Adoption of legislation.....	22
3. Awareness raising.....	24
4. Capacity building.....	28
5. Prevention of offending and re-offending.....	30
6. Research, data collection and monitoring.....	32
7. Law enforcement investigations.....	34
8. Reporting online child sexual abuse and exploitation.....	38
9. Assistance and protection measures for victims.....	42
10. Industry engagement.....	46
ANNEX: LEGISLATION ON ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION.....	49
I. International and regional legal framework.....	50
II. Status of REPERES Programme Countries.....	57
ENDNOTES.....	61

ACRONYMS

ACERWC	African Committee of Experts on the Rights and Welfare of the Child	INHOPE	International Association of Internet Hotlines
ACRWC	African Charter on the Rights and Welfare of the Child	IOCTA	Internet Organised Crime Threat Assessment
ASP	Access Service Provider	ISP	Internet Service Provider
C-PROC	Cybercrime Programme Office of the Council of Europe	ITU	International Telecommunications Union
CRC	Convention on the Rights of the Child	IWF	Internet Watch Foundation
CSA	child sexual abuse	MENA	Middle East and North Africa
CSE	child sexual exploitation	MNR	Model National Response
CSEC	commercial sexual exploitation of children	NCMEC	National Center for Missing and Exploited Children
EC3	European Cybercrime Centre	NGO	non-governmental organisation
ECPAT	End Child Prostitution, Child Pornography and Trafficking of Children for sexual purposes	NPA	national action plan
EFC	European Financial Coalition against Commercial Sexual Exploitation of Children Online	NSPCC	National Society for the Prevention of Cruelty to Children
EU	European Union	OPSC	Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography
FCACP	Financial Coalition Against Child Pornography	SGSM	self-generated sexual material
ICMEC	International Centre for Missing & Exploited Children	UK	United Kingdom
ICSE database	International Child Sexual Exploitation database	UN	United Nations
ICT	information and communication technology	UNICEF	United Nations Children's Fund
ILO	International Labour Organization	URL	uniform resource locator
		USA/US	United States of America
		VGT	Virtual Global Taskforce

INTRODUCTION

The Internet and other information and communication technologies have become an integral part of today's society, for both adults and children. Children especially spend many hours a day online, using numerous digital devices³ for a wide variety of activities (schoolwork, social networking, gaming, sharing pictures and videos, etc.). The online world helps us to connect with others and provides access to a colossal amount of information, which can be extremely useful for children's learning and development. Children do exercise some of their rights in the digital environment. However, just as there are risks in the offline world, there are also risks in the online world. These risks are associated with human behaviour. ICTs are legitimate tools or platforms that are used by perpetrators to facilitate the sexual abuse or exploitation of children. They do not cause the abuse or exploitation but severely aggravate its impact on the victims. Some of the features and characteristics of these platforms and tools, such as encryption or TOR, provide a false sense of anonymity to individuals who have a sexual interest in children. Children can also become more vulnerable in their capacity as Internet users, as research shows⁴ that they can engage in risky behaviour which in turn can make them an easy target for predators who are searching for potential victims in the online world.⁵

We must also acknowledge that the way in which technologies are misused varies tremendously depending on the form of online child exploitation and abuse, and that the most vulnerable children such as street children, those living in shelters, sexual slaves, and children being sexually abused in their homes, remain those most at risk. It is not the child's level of connectivity which defines his level of vulnerability but rather a series of personal and family circumstances, as well as his community environment, socio-economic factors and the predator's situation.

A child in the online environment is no different from a child offline and deserves the same level of protection. All persons under the age of 18 years are entitled to special protection. The impact of sexual exploitation and sexual abuse online is as serious as it is offline, and in some cases has even more severe consequences. For example, the online dissemination of child sexual abuse images can continue long after the victim has become an adult. Such material is recognised as "*the re-victimisation of the child by serving as a permanent record of abuse*"⁶ and the knowledge that the image or film can be repeatedly viewed and may never be removed causes ongoing trauma to the victim.⁷

According to law enforcement sources, the volume of child sexual abuse images circulating is believed to be very high, although no exact numbers can be provided. Furthermore, victims portrayed in the images are sometimes very young and the images depict different types of abuse, including the most severe such as penetrative sex and/or torture. INHOPE, the International Association of Internet Hotlines,⁸ noted an increase of 63% in the number of URLs containing child sexual abuse material reported to INHOPE between 2012 and 2014. INHOPE hotlines around the world received more than 1.5 million reports of illegal content in 2014 of which 57% was confirmed to be child sexual abuse material:⁹ 21% contained images depicting pubescent children, 72% depicted pre-pubescent children, and 7% infants.¹⁰

With regard to the most common geographical origin of the children in the images and videos, some research findings show that the majority of them are of Caucasian origin, 66.5% coming from Europe, 47.6% from North America, 29.1% from Asia, 5.9% from South America, 1.2% from Africa, and 1.2% from Oceania.¹¹ “[W]hat drives the production of child sexual abuse material is the internet infrastructure and technology in a specific country. In Europe and the USA, internet access is widespread and technology is highly developed. Therefore, that is where we see the largest share of material coming from. [...] The results do not indicate that there is less child sexual abuse in some parts of the world. They only reflect that the abuse is not documented and shared to the same extent. The more new technology and internet connectivity develops around the world, the more material we will see from Africa, Asia and South America.”¹² In other words, low internet coverage in Africa, with only 27.7% of the African population using the Internet,¹³ should not by any means be interpreted as meaning that a reduced number of children are victims of sexual abuse or exploitation in this region.

Many African countries are rapidly adopting cybercrime legislation and criminalising computer-facilitated sexual crimes against children, while in others, laws are weak, inconsistent or inexistent. However, even where legislation is in place, implementation sometimes remains a challenge.

The following examples¹⁴ illustrate some of the main vulnerabilities and threats:

- Self-generated sexual material (including sexting) is becoming increasingly widespread: For example, films of a sexual nature involving young girls have been found in **Burkina Faso** and there is evidence that they were self-produced by young students in Ouagadougou who later circulated them via mobile phones and the Internet.¹⁵ In **Uganda**, children that visit Internet cafes sometimes log into chat rooms to search for “clients” from different parts of the world in order to market their services.¹⁶
- The production of child abuse material is sometimes organised for purely commercial purposes, often with no prosecution of the offenders. In **Tanzania**, for example, there are reports that the production of child sexual abuse material is coordinated and organised in a professional manner, in part by Europeans.¹⁷ Various NGOs have revealed that tabloid newspapers and magazines (known as “udaku” in Kiswahili), have published “sexualised” pictures of children and that no legal action was taken against them, even though it is prohibited by law.¹⁸ In Kampala, **Uganda**, the production of child abuse material seems to be profit-driven, involving well-coordinated networks comprised of music celebrities as well as bar and karaoke group owners. It is estimated that almost 1,800 children are exploited every week through this form of commercial sexual exploitation.¹⁹

The need for action against online child sexual abuse and exploitation at the national level is imperative. However, as access to the Internet is universal and online child sexual abuse and exploitation is a global crime, a global response is also required.

This report aims to present and to define the different forms of online child sexual abuse and exploitation, to provide an overview of international cooperation and efforts to harmonise terminology and legislation, as well as to provide examples of good practice, particularly those that may be relevant for the countries targeted by the REPERES programme.

SECTION 1

DEFINING ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION

The world is changing. Technology provides more tools, but also presents new risks. Children's behaviour in the digital age is evolving and can increase their vulnerability. New forms of abuse are emerging and with them the need for new and accurate terminology.²⁰

Online child sexual abuse and exploitation is a problem that requires urgent attention. Since crimes committed online transcend borders, combating cybercrime requires international cooperation. Therefore, a common language is essential and definitions should be harmonised in order to develop a universal understanding of the real nature of the problem. This requires developing appropriate terminology and describing the constitutive elements of the different forms of abuse and exploitation, as well as their legal status. Furthermore, in order to understand the role played by ICTs in the process of exploiting and abusing a child, it is first necessary to define these acts in the offline world as well as to identify who is at risk.

1. CHILDHOOD AND THE AGE OF SEXUAL CONSENT

Child

Childhood entails a person's development from birth to adulthood. A child may be described using biological criteria, such as physical development, psychological criteria such as maturity, or moral criteria such as consent. However, these criteria do not provide a stable definition of the term "child", as they vary from one child to another, from one society to another. For instance, some children may reach puberty at the age of 10, while others reach it at the age of 14 or 15. Moreover, different perceptions regarding childhood and maturity exist in different cultures and contexts.

Children ensure the future sustainability and development of our society but are also one of its most vulnerable groups and as such, require additional protection. In order to ensure that no child is denied her/his right to protection, this protection cannot depend on the use of variable or subjective criteria. As a result, lawmakers around the world have decided to use age as the sole criterion and as such, international legally binding instruments define a child as any person under the age of 18 years.²¹

Age of sexual consent

The age of sexual consent is legally defined as the age below which it is prohibited to engage in sexual activities with a child.²² However, no international treaty establishes the legal age for sexual activities, leaving it up to the States to legislate on the matter. Although it varies from country to country, many set the age of sexual consent at between 14 and 16 years of age.

While a person under the age of 18 may be able to freely consent to sexual relations, such an individual is not legally able to consent to any form of sexual exploitation²³ or abuse. It is therefore important that States criminalise all forms of sexual exploitation up to the age of 18 years, and consider any presumed "consent" to exploitative or abusive acts as null and void.²⁴

2. CHILD SEXUAL ABUSE AND CHILD SEXUAL EXPLOITATION

Child sexual abuse

Article 18(1) of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)²⁵ defines child sexual abuse as “*engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities*”²⁶ and “*engaging in sexual activities with a child where: use is made of coercion, force or threats; or abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.*”

The sexual abuse of children requires no element of exchange, and can occur for the sole purpose of the perpetrator’s sexual gratification. Such abuse can be committed without explicit force, with other elements, such as authority, power, or manipulation being determining factors. Moreover, it is noteworthy that, when the child has not reached the age of sexual consent, there is no legal requirement to establish any of these elements. The mere fact of the sexual activity taking place is sufficient to constitute abuse. Child sexual abuse (CSA) is a broad category that, at its core, defines the harm caused to children by forcing or coercing them to engage in sexual activity, whether they are aware of what is happening or not.²⁷

Child sexual abuse can take the form of both contact and non-contact abuse, the latter committed without physical contact with the child. Examples of non-contact sexual abuse are activities “*involving children in looking*

at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet).”²⁸

Child sexual exploitation

Child sexual exploitation (CSE) is a type of sexual abuse. A child is a victim of sexual exploitation when she/he takes part in a sexual activity in exchange for something (gain, benefit, or even the promise of such) from a third party, the perpetrator, or by the child her/himself. Therefore, what distinguishes the concept of child sexual exploitation from other forms of child sexual abuse is the underlying notion of exchange.²⁹

Children or young people³⁰ may be coerced into a situation of sexual exploitation through physical force or threats. The perpetrator may take advantage of additional factors that make a child vulnerable, such as poverty or neglect. For example, there are cases where sexual exploitation occurs in exchange for protection, a place to sleep, or access to higher grades and/or promotion. Older children may be tricked into believing they are in a loving, consensual relationship.

The term “child sexual exploitation” has been defined by many legally binding instruments. For example, the African Charter on the Rights and the Welfare of the Child (ACRWC)³¹ refers to “*all forms of sexual exploitation and sexual abuse*”, and explicitly mentions in Article 27 “(a) *the inducement, coercion or encouragement of a child to engage in any sexual activity; (b) the use of children in prostitution or other sexual practices; (c) the use of children in pornographic activities, performances and materials*”. Furthermore, the European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography (Directive 2011/93/EU)³² defines

offences concerning sexual exploitation in its Article 4, and includes in that definition acts such as making a child participate in pornographic performances, knowingly attending pornographic performances that include children, making a child participate in child prostitution, and engaging in sexual activities with a child where recourse is made to prostitution.³³

Finally, it should be noted that, even if child sexual abuse and child sexual exploitation are two different phenomena, there are cases where the distinction is not clear. For example, some cases of child sexual abuse may also involve some kind of benefit to the child or exchange — often to win trust or ensure silence (especially non-tangible benefits such as attention or affection). Similarly, the idea of exploitation is arguably applicable to all victims of abuse in the sense of exploiting the vulnerability of a child.³⁴

3. ONLINE CHILD SEXUAL ABUSE AND ONLINE CHILD SEXUAL EXPLOITATION

Online child sexual abuse

Online child sexual abuse is any form of child sexual abuse, which has a link to the online environment.³⁵ For example, unwanted sexual comments made to a child through social media is a form of online child sexual abuse³⁶ as is uploading and making images or videos of sexual abuse available online. Children can be at risk of online abuse from people they know, as well as from strangers.

Online abuse may be part of abuse that is taking place offline and is facilitated by information and communication technologies (ICTs), for instance an adult may groom a child online with the intention of abusing her/him physically; the abuse may be committed elsewhere and then repeated by sharing it online through, for example, images and videos;³⁷ or it may be that the abuse only happens online, for instance by persuading children to take part in sexual activity online.³⁸

Online child sexual exploitation

As with child sexual abuse, child sexual exploitation can also occur both online and offline. Thus, the term “online child sexual exploitation” refers to the use of the Internet as a means to exploit children sexually.³⁹ When sexual exploitation takes place online, the child may be persuaded/threatened/forced to take part in sexual activities via a smartphone or in front of a webcam, to participate in sexual conversation or to send sexual pictures of themselves. Abusers may threaten to send images, video or copies of conversations to the young person’s friends and family unless they take part in further sexual activity.⁴⁰

Furthermore, perpetrators may identify and/or groom potential victims online with a view to exploiting her/him sexually, whether or not the acts that follow are carried out online or offline. Other forms of online child sexual exploitation are the distribution, dissemination, importing, exporting, offering, selling, possession of, or knowingly obtaining access to child sexual exploitation material online, even if the sexual abuse depicted was committed offline.⁴¹

Commercial sexual exploitation of children (CSEC) is a form of child sexual exploitation, which involves primarily monetary exchanges. In the online environment, the purpose of the monetary benefit or the nature of “commercial” may vary.

In the context of the European Financial Coalition (EFC),⁴² *“[t]he use of the word commercial refers to child abuse images that are available to purchase. This could include a website designed to provide child abuse images for a cost (normally subscription), or uncensored newsgroups who charge a fee for membership and have child abuse images available as part of their service.”* It could also include the re-selling of images, or requiring paid access to online facilities such as linked pages or cyberlockers, which can be used by offenders to store or distribute their images.⁴³

Even if the commercial distribution of child abuse images and videos is largely profit driven and conducted by criminals with a limited sexual interest in children, the commercial nature of such distribution also exists among those having such an interest, when for instance, child abuse material is exchanged not for monetary gain but for other child sexual abuse material. In this case, the material itself becomes the currency.

Developments such as profit driven blackmailing of young people to disseminate sexually explicit photos or videos depicting themselves, as well as the commercial distribution of images and videos obtained as self-generated sexual exploitation material, should also be taken into consideration in order to complete the current picture of commercial child sexual exploitation.⁴⁴

4. CHILD SEXUAL ABUSE MATERIAL AND CHILD SEXUAL EXPLOITATION MATERIAL

Child sexual abuse material, child sexual exploitation material or “child pornography”

“Child pornography” is the legal term that describes child sexual abuse material, but also the offences of producing/preparing, consuming, sharing/spreading/disseminating, or possessing such material.⁴⁵ For instance, the Optional Protocol to the Convention on the Rights of the Child (CRC) on the sale of children, child prostitution and child pornography (OPSC)⁴⁶ defines child pornography in Article 2(c), as “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes”⁴⁷ and requests, in Article 3(1) (c), States to criminalise the following acts: “[p]roducing, distributing, disseminating, importing, exporting, offering, selling, or possessing for the above purposes child pornography.” A narrower definition but a broader range of prohibited acts are included in the Lanzarote Convention, which, in Article 20(1 and 2), defines child pornography as “any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes” and prohibits “producing child pornography; offering or making available child pornography; distributing or transmitting child pornography; procuring child pornography for oneself or for another person; possessing child pornography; [and] knowingly obtaining access to child pornography”.⁴⁸

Although the term “child pornography” is used by international treaties and national laws, it

fails to describe the gravity of the acts and the damage these acts cause to children.

As stressed by INTERPOL,⁴⁹ “[c]hildren who have been sexually abused and photographed or filmed deserve to be protected and respected, and not have the seriousness of their abuse reduced by the use of terms such as “porn”. Pornography is a term used for adults engaging in consensual sexual acts distributed (mostly) legally to the general public for their sexual pleasure. Child abuse images involve children who cannot and would not consent and who are victims of a crime. Terms such as “kiddy porn” and “child porn” are used by criminals and should not be legitimate language used by law enforcement, judiciary, the public or media.”⁵⁰

This has been the general approach of the law enforcement sector in recent years, and it has led the way in characterising “child pornography” as documented evidence of a crime in progress — a child being sexually abused. Law enforcement bodies in many countries, as well as Europol⁵¹ and INTERPOL at the international level, and child protection agencies thus tend to reject the term “child pornography” and use either “child sexual abuse material” or “child sexual exploitation material”,⁵² terms that highlight the abusive or exploitative aspects of this phenomenon.⁵³ Legislation that accurately defines the offences and affords better protection and rights to victims should follow. As a result, society as a whole would develop a better understanding of the seriousness of these crimes, which may also contribute to their prevention.

Child sexual abuse material (CSAM) is material depicting acts of sexual abuse and/or focusing on the genitalia of the child, while child sexual exploitation material (CSEM) is used in a broader sense to encompass all other sexualised material depicting children.⁵⁴ CSAM/CSEM include the following cases:

- It includes visual material such as photographs, movies, drawings, and cartoons; audio representations; live performances; written material in print or online; and physical objects such as sculptures, toys, or ornaments.⁵⁵
- It includes not only children but also adults “*appearing to be*” children.⁵⁶
- Child sexual abuse/exploitation material is also “*pornographic material consisting exclusively of simulated representations or realistic images of a non-existent child*”, known as “virtual child pornography”.⁵⁷
- Self-generated sexual material could be CSAM/CSEM under certain circumstances.⁵⁸
- Sexualised images of children could be CSEM under certain circumstances.⁵⁹

Computer / digitally generated child sexual abuse material or “virtual child pornography”

The term “computer (or digitally) generated child sexual abuse material” encompasses all forms of material representing children involved in sexual activities and/or in a sexualised manner, with the particularity that the production of the material does not involve the abuse of real children but is artificially created to appear as if real children were being abused. It is also referred to as “virtual child pornography” or “pseudo child pornography” and can include, but is not limited to, “pseudo photographs”,⁶⁰ comics, drawings, cartoons and full movies of child sexual abuse that do not involve real children. Although most artificially created child sexual abuse material is computer-generated, it is important to note that such material can also include pictures drawn by hand.⁶¹

Although computer-generated child sexual abuse material does not necessarily involve direct physical harm to a child in its creation, it is still harmful because (i) it is known to be used in grooming children for exploitation; (ii) it fuels very real fantasies, encourages the propensity of sexual predators, and contributes to maintaining a market for child sexual abuse material; and (iii) it creates a culture of tolerance for the sexualisation of children and thereby cultivates demand.⁶²

As a result, computer/digitally generated child sexual abuse material constitutes a serious offence against children. It should thus be illegal in all jurisdictions.

At the international level, this type of material is covered by the Council of Europe Convention on Cybercrime (Budapest Convention)⁶³ in Article 9(2)(c), and Directive 2011/93/EU, in Article 2(c)(iv), and referred to by these legal instruments as “*realistic images of a child engaged in sexually explicit conduct*”.⁶⁴ At the national level, in the United Kingdom (UK) for instance, pseudo child pornography is treated identically to child sexual abuse material depicting real children, except with regard to sentencing for the offence, which may be lighter in the case of pseudo child pornography.⁶⁵

The term “virtual” frequently used in this context should not be confused with “existing online”, because, although it does indeed exist online, it refers to images that have been created with the purpose of conveying the impression that they depict children. There is nothing “virtual” or unreal in the sexualisation of children and these terms risk undermining the harm that children can suffer from these types of practices or the effect that material such as this can have on the cognitive distortions of offenders or potential offenders. Thus, the term “virtual” should be avoided.⁶⁶

Self-generated sexual material

Law enforcement agencies report that self-generated sexual material (SGSM) is a current trend, the “*commodity of ‘newly produced never before seen’ CSAM to be used as a currency in further trade*”,⁶⁷ accounting for its growing volume in circulation.⁶⁸ One factor reportedly responsible for the increase of SGSM is the proliferation of mobile phones and social network applications available on mobile phones. In essence, the more common and popular the mobile app, the more likely an increase in abuse material being transmitted.⁶⁹

The problem also arises from how willing young people are to show themselves naked on webcam.⁷⁰ Some national law enforcement agencies have observed that children are becoming more daring and explicit, and often more complicit in terms of self-generated sexually “explicit” images⁷¹ with 85.9% of content depicting children aged 15 or younger being created using a webcam in a home environment, most commonly a bedroom or bathroom,⁷² as reported by the Internet Watch Foundation (IWF).

The NetClean Report 2016 defines self-generated sexual material as follows: “*This can be nude or undressed images and videos that the children themselves have taken, either voluntarily or as a result of coercion. It can be nude images that youths send to a girlfriend/boyfriend or upload onto the Internet seeking affirmation, usually without understanding or thinking of the risk of the images spreading. But it is also about children that have been groomed and then coerced or blackmailed into sending images and videos of themselves.*”⁷³

Cases of SGSM can be divided into two categories: SGSM created within the context of a romantic relationship between consenting older teenagers, and SGSM featuring younger children.

Regarding the first category, even when self-generated sexual material is created with consent,⁷⁴ it presents significant risks. For example, the self-generated content can fall into the wrong hands and end up being distributed within the context of grooming and online solicitation, including sexual extortion. As a result, SGSM, illegal or not depending on the jurisdiction, can be very harmful.⁷⁵

Regarding the second category, when SGSM features younger children, it is possible that another person has dictated the sexual acts depicted and the reasons behind its production are potential coercion or manipulation. For any SGSM depicting a younger child, the assumption ought to be that it is the result of an abusive or coercive relationship with an adult or another child.⁷⁶ As a result, abuse or exploitation is involved and this form of SGSM should be considered as CSAM/CSEM and be illegal.

Although children (in particular adolescents) may willingly produce sexual content, this does not mean they consent to or are responsible for the exploitative or abusive use and/or distribution of these images. Therefore, they should never face criminal liability for their role in producing or making available the material.⁷⁷ Nevertheless, in some jurisdictions it continues to be the case that the child who generated and distributed the picture is guilty of producing and disseminating CSAM.⁷⁸

Sexting

“Sexting” has been defined as the “self-production of sexual images”, or as the “exchange of sexual messages or images” and “the creating, sharing and forwarding of sexually suggestive nude or nearly nude images through mobile phones and/or the internet”.⁷⁹ Various reasons explain why children engage in sexting: joining in because they think that “everyone is doing it”; boosting their self-

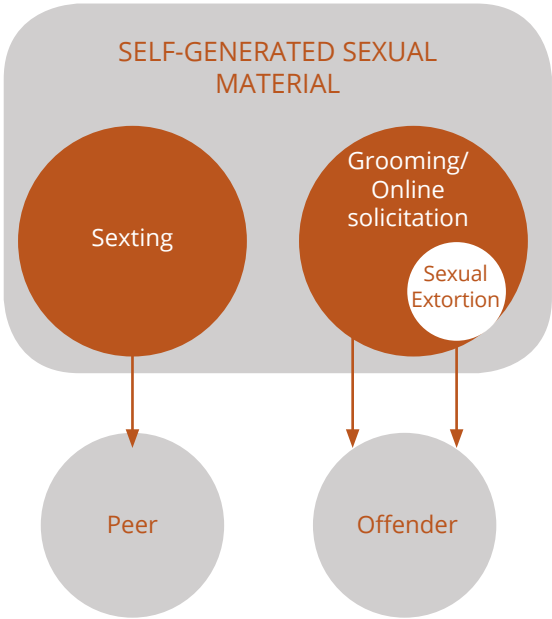
esteem; flirting with others and testing their sexual identity; exploring their sexual feelings; to get attention and connect with new people on social media; they may find it difficult to say no if somebody asks them for an explicit image, especially if the person asking is persistent.⁸⁰

As a result, sexting can be perceived as “harmless fun”,⁸¹ often carried out between consenting adolescents who derive pleasure from the experience. However, it can also be “unwanted” such as sharing or receiving unsolicited sexually explicit photos, videos, or messages, or even take the form of sexual cyber-bulling, where a child is pressured to send a picture to a boyfriend/girlfriend/peer, who then distributes it to a peer network without their consent.⁸²

Sexting is a form of self-generated sexual material, not a synonym. The recipients of SGSM produced through sexting are generally peers. The recipients of SGSM produced in other contexts such as grooming and online solicitation, including sexual extortion, are offenders.⁸³ When sexting leads to abuse or exploitation, it is crucial that the fact that the material is self-generated does not result in blaming the child for what happened or in holding the child criminally liable for the production of child sexual abuse material.⁸⁴

As reported in a survey conducted by Missing Children Europe, ECPAT and eNASCO,⁸⁵ the UK is the only EU Member State to have passed a new law in addition to the law on grooming, introducing the offence of sexting,⁸⁶ which states that it is illegal for an adult to communicate sexually with a child under the legal age of consent in view of the sexual gratification of the adult.

Comparison between self-generated sexual material and sexting:⁸⁷



Sexualised images of children

Sexualised images of children are images of children posing semi-nude or nude with an emphasis on sexualisation. Such images could be, for instance, a family picture of a young child in a bikini or in her mother's high heels. Other images may have been deliberately staged to sexualise the child depicted. Sexualisation is not always an objective criterion, and the crucial element in judging such a situation is the intent of a person to sexualise a child in an image or to make use of an image for sexual purposes (e.g. for sexual arousal or gratification).

Since this material does not depict children engaged in explicit sexual activities or conduct, it does not fall under the legal definition of "child pornography", the question that arises is whether or not sexualised images of children should be illegal and if so, under what circumstances. Even if such images were not initially produced for sexual purposes, they may pose some risks: They can be circulated within (online) networks of people with a sexual interest in children, and serve to underpin the belief of some persons that the sexualisation of children is normal; In criminal investigations and court rulings on child sexual exploitation, it has been proven that websites publishing sexualised images of children are sometimes used as a first step to, and can serve to cover up the sexual exploitation of children, as well as being used in the grooming process.⁸⁸

As a result, sexualised images of children are generally not considered illegal, as they do not necessarily depict sexual abuse. However, their distribution could be considered as CSEM and thus illegal. Moreover, the distribution of the images may constitute a serious violation of the right to privacy of the child (or later of the adult person).⁸⁹

5. LIVE ONLINE CHILD SEXUAL ABUSE

Live online child sexual abuse

Live online child sexual abuse is a practice on the rise. It is related to the sexual exploitation of children through prostitution and sexual performances as well as to the production of child sexual abuse material. Given the absence of a clear definition of this practice as an offence, this field has seen an absence of adequate criminalisation. However, while not explicitly included in major international legal instruments addressing child protection, it is crucial to note that live online child sexual abuse would fall under many existing legal provisions related to child sexual exploitation and sexual abuse.⁹⁰

Live online child sexual abuse often represents a dual abuse of the child. She/he is coerced to participate in sexual activities, alone or with other persons — an act that already constitutes sexual abuse. The sexual activity is, at the same time, transmitted live through ICT and watched by others remotely. Forms of live online child sexual abuse vary in the way the sexual activity is transmitted over the Internet ("live streaming of child sexual abuse/on-demand child sexual abuse") and how it is carried out ("child sexual abuse to order"). Live online child sexual abuse has been observed to take on both commercial and non-commercial forms, and there are cases where it has been set up as a business with the only apparent objective being to make money out of the sexual exploitation of the children involved.⁹¹

Live streaming of child sexual abuse/on-demand child sexual abuse

The live streaming of child sexual abuse on the internet entails the sexual activity being

transmitted instantaneously to the viewer, who can watch and engage while the abuse is occurring. The live abuse of children is pre-arranged according to a specific time frame through video sharing platforms.⁹² Importantly for the viewer, streaming leaves no trace on the device, because no file is downloaded; when the streaming is stopped the child sexual abuse material is gone, unless the offender deliberately records it.⁹³

Live streaming of child sexual abuse/on-demand child sexual abuse is a key threat⁹⁴ and one of the key challenges faced by police officers working on child sexual abuse cases.⁹⁵

The increasing Internet coverage in developing countries has had an impact on online child sexual exploitation in their jurisdictions.⁹⁶ Law enforcement agencies around the world report that the majority of victims of live-streamed abuse over the Internet are based in South-East Asia, in particular the Philippines. In general, however, offenders — almost all perpetrators are from Europe and the USA — are targeting regions of the world with high levels of poverty, limited domestic child protection measures and easy access to children, for all types of child sexual exploitation material, including live streaming.

Links between the live streaming of child sexual abuse and subsequent travelling for the purpose of child sexual exploitation have also been identified.⁹⁷

Child sexual abuse to order

“Child sexual abuse to order” refers to a specific type of online sexual abuse that consists of a perpetrator requesting or dictating the performance of certain sexual activities, either before or during the abuse. The abuse is displayed via webcam or recorded to a file for the viewing/consumption of the person who ordered it, sometimes in exchange for payment.⁹⁸

6. SOLICITATION OF CHILDREN FOR SEXUAL PURPOSES

Online grooming

The solicitation of children for sexual purposes is often referred to as “grooming” or “online grooming”. It can be described as a practice by means of which an adult “befriends” a child (often online, but also offline) with the intention of sexually abusing her/him.⁹⁹

Online grooming in particular refers to the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with a child. The process of grooming includes actions taken by the offender (for example through email, social media, gaming systems, chatting) to build a relation of trust with the child and possibly arrange a face-to-face meeting. As the relationship develops, child sex offenders may show pornography (involving adults or children) to the victim in order to lower the child’s inhibitions, to normalise and desensitise the child to sexual activity, as well as to teach the child sexual behaviours. Showing pornographic images and videos to the child can also increase the child’s sexual curiosity and lead to sexual discussions that may advance a sexual relationship and ultimately increase the likelihood of a sexual encounter, physical or virtual, with that child.¹⁰⁰ Solicitation of children for sexual purposes may never go offline. In such cases, the reason for online grooming may be the offender’s sexual gratification through non-contact offences,¹⁰¹ blackmailing of the victims, or the production of child sexual abuse material. Whether or not a face-to-face meeting occurs, the harm caused to the victims is serious. They often have to deal with feelings of shame and guilt for having, to some extent, contributed to their own exploitation (e.g. because initially they agreed to turn on their webcams and/

or take photos), as well as the anxiety of permanently losing control of the images and not knowing who has seen them.¹⁰² As a result, legislation should criminalise all forms of grooming, offline and online, with or without the intention of entering into physical contact with the victim.¹⁰³ Only through this approach can children be protected effectively. As the Explanatory Memorandum for Ireland's Criminal Law (Child Grooming) Bill 2014 sets forth, *"if a meeting or steps towards a meeting is required, it may be too late to avert the threat to the child in question, even though grooming has already occurred."*¹⁰⁴

Sexual extortion of children

Sexual extortion is considered a feature of online solicitation. It involves a process whereby children or young people are coerced into continuing to produce sexual material under the threat of exposing the said material to others (for example posting images on social media). The offender blackmails the child in order to obtain sexual gratification or money. The latter is called "commercial sexual extortion", in which case the offenders look for an easy way to obtain financial gain. This can take the form of either blackmailing the victims by demanding money in exchange for not distributing the sexually explicit material depicting them, or the commercial distribution of material obtained through online solicitation.

Often, the influence and manipulation typical of groomers over longer periods of time (sometimes several months) turns into a rapid escalation of threats, intimidation, and coercion once the child has been persuaded to send the first sexual images of her/himself. In some instances, the abuse spirals so out of control that victims have attempted to self-harm or commit suicide as the only way of escaping it.

There is some evidence pointing to a ring of African states, in addition to the Southeast Asia based networks, targeting victims throughout Europe.¹⁰⁵



In July 2013, a 17-year-old boy died when he threw himself from a bridge near Edinburgh. He had been targeted online by an offender who posed as a teenage girl and with whom he shared sexually explicit images of himself. The victim was then blackmailed by the offender demanding money. If he failed to pay, he would post the victim's naked images on social networking sites.¹⁰⁶

Exposure to pornography and corruption of children for sexual purposes

Exposure to harmful content refers to children accessing or being exposed to, intentionally or incidentally, age-inappropriate sexual or violent content, or content otherwise considered harmful to their development. The harmful content could include adult pornography and child sexual abuse material.¹⁰⁷


Exposure to pornography contributes to the increasing sexualisation of children in society, which can contribute to normalising sexual behaviours and attitudes among young children.¹⁰⁸ Maggie Atkinson, former Children's Commissioner for England has said, *"We are living at a time when violent and sadistic imagery is readily available to very young children, even if they do not go searching for it, their friends may show it to them or they may stumble on it whilst using the internet. We all have a duty to protect children from harm – it is one of their rights enshrined in the United*

*Nations Convention on the Rights of the Child – and the time has come for immediate and decisive action to do so. For years, we have applied age restrictions to films at the cinema but now we are permitting access to far more troubling imagery via the internet. We do not fully understand the implications of this. It is a risky experiment to allow a generation of young people to be raised on a diet of pornography.*¹⁰⁹

As a result, children are becoming accustomed to pornographic content that may encourage them to engage in sexual activity at an earlier age, unaware of the risks, or result in an increased level of sexual aggression between minors.¹¹⁰

Exposure of children to pornography may be used to lower child's inhibitions or to increase a child's sexual curiosity, for example, as part of the process of grooming or sexual extortion. It is sometimes referred to as the "corruption of children for sexual purposes", when children are intentionally caused to witness sexual abuse or sexual activities, which is illegal.¹¹¹ Some state laws in the US use the term "online sexual corruption of a child" as an alternative to grooming.¹¹²

An adult deliberately showing pornography to a child constitutes a form of non-contact sexual abuse.¹¹³

A grayscale photograph of a hand using a computer mouse, positioned on the left side of the page. The background is a dark, vertical gradient.

SECTION 2

GOOD PRACTICE FOR PROTECTING CHILDREN AGAINST ONLINE SEXUAL ABUSE AND EXPLOITATION

This report considers good practice to be any measure that strengthens the protection of children from online child sexual abuse and exploitation and that ensures justice for its victims. Examples include legislative measures that contain provisions for effective investigation and prosecution of crimes, services for victims, policy rules and guidelines, cross-border and cross-sectoral cooperation, awareness raising and capacity building programmes. An integrated approach combining the aforementioned good practice is the most effective means of combating the sexual exploitation of children.

This section outlines good practice as well as a series of initiatives developed by stakeholders around the world, both from the public and private sector (governments, law enforcement agencies, judiciary, international organisations, civil society, and industry), in order to protect children against online sexual offences.

1. NATIONAL ACTION PLAN

A national action plan (NAP) is a coordinated national response to a specific issue. In the context of online child sexual abuse and exploitation, a NAP can be either part of a broader child protection plan or a specific plan addressing online child sexual abuse and exploitation. A NAP provides a comprehensive, long-term blueprint for a country seeking to prioritise this issue in its political, social and legislative agendas. As such, it is a valuable tool for helping relevant stakeholders across all sectors to understand the scope of the issue and establish cohesive policies, procedures, standards, mechanisms, technologies, and other resources to address it.¹¹⁴ All examples of good practice identified in this document could be used to form the basis of a national action plan.








A well-constructed NAP highlights that online child sexual abuse and exploitation cannot be addressed by only one actor or country; it requires the participation of stakeholders from both the public and private sector as well as coordinated action and communication through the sharing of knowledge and resources.

A NAP should provide a holistic approach, tailored to the national context (e.g. needs, feasible solutions) whilst also respecting international standards and contributing to international cooperation. Furthermore, it should also enable a country to monitor and assess its response, identify new trends and weaknesses and update it accordingly. The establishment of a national body¹¹⁵ comprising representatives from different sectors (e.g. law enforcement, civil society, industry) and responsible for coordinating and monitoring the NAP would further strengthen these aspects. The function of such a mechanism could include the submission of annual reports, surveys among victims, the identification of challenges related to implementation of the law as well as legal opinions and proposals. Finally, this role could also include exchanging information on legal and technological developments in addition to good practice with other countries. In doing so, international cooperation is facilitated and the country in question improves its capacity to prevent and tackle the sexual abuse and exploitation of children online.



The WePROTECT Global Alliance to End Child Sexual Exploitation Online is an international movement dedicated to national and global action to end the sexual exploitation of children online.¹¹⁶ This initiative helps countries to strengthen their response to online child sexual exploitation with the “Model National Response” (MNR). The MNR describes the capabilities required for effective child protection, highlights good practice from countries that are already delivering these capabilities, and indicates organisations that can provide further guidance and support to countries seeking to develop or enhance their existing capability.¹¹⁷ As a result, the MNR can be used as guidance for countries that have not established a national action plan or for those that need to improve it. 70 countries are already members of the WePROTECT Global Alliance, including Rwanda and Uganda, along with major international organisations, 20 technology companies, and 17 leading civil society organisations. Its members share the commitment to put an end to online child sexual exploitation, by identifying and protecting victims, removing child sexual abuse material from the internet and tracking down the perpetrators of this abuse.

Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response¹¹⁸

Enablers	Capabilities	Outcomes	
Cross sector, multi-disciplinary collaboration	Policy and Governance 	1 Leadership: An accountable National Governance and Oversight Committee	Highest level national commitment to CSEA prevention and response Comprehensive understanding of CSEA within the highest levels of government and law enforcement. Willingness to work with, and co-ordinate the efforts of, multiple stakeholders to ensure the enhanced protection of victims and an enhanced response to CSEA offending.
		2 Research, Analysis and Monitoring: National situational analysis of CSEA risk and response, measurement/indicators	
		3 Legislation: Comprehensive and effective legal framework to investigate offenders and ensure protection for victims	
Willingness to prosecute, functioning justice system and rule of law	Criminal Justice 	4 Dedicated Law Enforcement: National level, trained officers; proactive and reactive investigators; victim-focused; international cooperation	Effective and successful CSEA investigations, convictions and offender management Law Enforcement and judiciary have the knowledge, skills, systems and tools required to enable them to perform victim-focused investigations and secure positive judicial outcomes. CSEA offenders are managed and reoffending prevented.
		5 Judiciary and Prosecutors: Trained, victim-focused	
		6 Offender Management Process: Prevent re-offending of those in the criminal justice system nationally and internationally	
		7 Access to Image Databases: National database, link to Interpol database (ICSE)	
Supportive reporting environment	Victim 	8 End to End Support: Integrated services provided during investigation, prosecution and after-care	Appropriate support services for children and young people Children and young people have access to services that support them through the investigation and prosecution of crimes against them. They have access to shelter, specialised medical and psychological services; and rehabilitation, repatriation and re-socialization services.
		9 Child Protection Workforce: Trained, coordinated and available to provide victim support	
		10 Compensation, remedies and complaints arrangements: Accessible procedures	
Aware and supportive public and professionals, working with and for children	Societal 	11 Child Helpline: Victim reporting and support, referrals to services for ongoing assistance	CSEA prevented Children and young people are informed and empowered to protect themselves from CSEA. Parents, carers, teachers and childcare professionals are better prepared to keep children safe from CSEA, including addressing taboos surrounding sexual violence.
		12 CSEA Hotline: Mechanism for reporting online CSEA content, link to law enforcement and internet service providers	
Sufficient financial and human resources	Industry 	13 Education Programme: For children/young people, parents/carers, teachers, practitioners, faith representatives	Industry engaged in developing solutions to prevent and tackle CSEA Industry has the power and willingness to block and remove online CSEA content and proactively address local CSEA issues. Industry proactively reports online CSEA.
		14 Child Participation: Children and young people have a voice in the development of policy and practice	
		15 Offender Support Systems: Medical, psychological self-help, awareness	
National legal and policy frameworks in accordance with the UNCRC and other international and regional standards	Industry 	16 Takedown Procedures: Local removal and blocking of online CSEA content	Awareness raised among the public, professionals and policy makers Potential future offenders are deterred. CSEA offending and reoffending is reduced.
		17 CSEA Reporting: Statutory protections that would allow industry to fully and effectively report CSEA, including the transmission of content to law enforcement or another designated agency	
		18 Innovative Solution Development: Industry engagement to help address local CSEA issues	
		19 Corporate Social Responsibility: Ethical child-focused programme	
Data and evidence on CSEA	Media and Communications 	20 Ethical and Informed Media Reporting: Enable awareness and accurate understanding of problem	
		21 Universal Terminology: Guidelines and application	

2. ADOPTION OF LEGISLATION

Adoption of legislation is the starting point as it provides a framework for protecting children against sexual abuse and exploitation as well as for bringing the perpetrators to justice, and outlines the roles and responsibilities of each member of society. Legislation enables reporting of sexual offences against children, investigative tools, prosecution, access to justice for the victims, preventive measures and a clean Internet. In order for legislation to be comprehensive and effective, it must be compliant with the standards set by international law and meet certain criteria.

INTERNATIONAL STANDARDS

Either by ratifying international treaties or (when ratification or accession is not possible) using international treaties as a model for drafting domestic legislation, countries should comply with and implement international legal standards as an initial step in addressing online child sexual abuse and exploitation. The Convention on the Rights of the Child (CRC)¹¹⁹ and its Optional Protocol, the Budapest Convention, the Lanzarote Convention and the Directive 2011/93/EU set international standards and good practice for child protection, in addition to promoting international cooperation for combating online child sexual abuse and exploitation.

CRITERIA FOR EFFICIENT LEGISLATION

- ✓ All forms of child sexual abuse and exploitation must be defined and criminalised, including the following:
 - knowing possession of child sexual abuse/exploitation material, regardless of the intent to distribute
 - knowingly obtaining access to CSAM/CSEM (downloading or viewing) on the internet
 - grooming either offline or online¹²⁰
 - sexting with a child for the purpose of exploiting her/him sexually¹²¹
 - offering information on where to find child sexual abuse/exploitation material.¹²²

- ✓ Children should not be criminalised regardless of whether she/he was a compliant victim or a non-cooperative witness in judicial proceedings. Criminal liability must focus on the adult offender and on the crimes committed against the child.¹²³ Children who have not reached the age of criminal responsibility should not be considered offenders under any circumstances.¹²⁴
- ✓ Extended statutory limitation period for sexual offences against children, which begins to run when the child reaches the age of 18.¹²⁵
- ✓ Data retention and/or preservation provisions in order to prevent loss or modification of stored computer data for a specific period of time so that it can be used as evidence during an investigation.¹²⁶
- ✓ Provisions for effective investigative tools, including offender and victim identification and undercover operations.¹²⁷
- ✓ Measures against websites containing or disseminating child sexual abuse and exploitation material¹²⁸ and mandatory reporting requirements for certain actors.¹²⁹
- ✓ Dual criminality¹³⁰ shall not be required for convicting offenders in a country for serious sexual crimes committed abroad against children.¹³¹
- ✓ Provisions for international cooperation with respect to the investigation and prosecution of child sexual abuse and exploitation.

3. AWARENESS RAISING

Awareness raising is essential for many reasons: children need to be aware of the dangers in order to avoid situations at risk; parents need to know how they can protect their children; teachers need to know how to protect their students; victims and members of society need to know how to report and obtain assistance; potential offenders may be dissuaded if they are aware of the law. Awareness raising¹³² can take many forms, be carried out by different actors and target different groups.



Parents need to understand the online environment, how their children use the Internet,¹³³ how to discuss online sexual behaviour with their children, how to avoid the risks, and, if their child becomes a victim of online child sexual abuse or exploitation, how to react and seek help. Support for parents could take the form of educational material, family workshops, counselling for parents, and helplines. This support could be provided by schools, parent associations, civil society groups or local/national authorities.



In Sweden for example, the National Institute of Public Health was assigned the responsibility to support parents with a wide range of resources as part of the National Action Plan for Safeguarding Children from Sexual Exploitation.¹³⁴

The role of parents

Parents can raise the awareness of their children and support them to become responsible users of technology. As a result, their children will be less vulnerable to online predators.

- **Establishing family rules and guidelines for safety and security:** House rules should be agreed with respect to use of the Internet and personal devices, lending particular attention to issues of privacy and age inappropriate websites and the location of computers.¹³⁵ For example, computers should be located in a common room as this reduces the chances of a child being contacted by predators, accessing online pornography, or producing compromising images of her/himself.¹³⁶ Moreover, the installation of software is recommended to allow parents to control some or all functions of a computer or other devices that can connect to the Internet. Such software can limit access to certain categories of websites or record all texts sent or received from a device.¹³⁷

- **Communication:** All over the world, many parents make the false assumption that their children are “safe” at home using their computer¹³⁸ and underestimate their exposure to risks online. Parental supervision is not simply monitoring the child’s online activities, but also involves creating an environment of trust and communication with their child. It means that parents should discuss safety rules with their children, read the terms and conditions of use with their children before they enter a website,¹³⁹ educate them on the risks associated with disclosing personal information when going online, arranging face-to-face meetings with a person they met online, posting photographs online, making use of the webcam.¹⁴⁰ It can also take the form of enjoying certain online activities together with their children such as interaction through social networks and gaming.¹⁴¹



Teachers should be familiar with ICTs, have a good understanding of how children use the Internet and then be able to teach children positive and responsible forms of online behaviour.¹⁴² Through quality education, children can also gain the skills and abilities to surf cyberspace with confidence, avoid and address risks, and become well-informed and responsible digital citizens. This includes promoting creative, critical and safe use of the Internet as well as preventing and responding to incidents of online violence.¹⁴³ Education dedicated to online child sexual exploitation and abuse could provide students and teachers with information about where to seek advice and support, as well as where to report abuse.¹⁴⁴ Therefore, schools and the education system could play a very important part in raising awareness:

- **For teachers:** Education programmes on ICT, internet safety policy and online child sexual abuse and exploitation issues.
- **For children:** Compulsory school curriculum on sexual development, sexual behaviour and internet safety.¹⁴⁵

It should be noted that, together with educational programmes, technical support should be provided to schools and teachers to further support children’s internet use and safety, including the establishment of filtering software to computers at schools, so that children are not able to access illicit content when using them or cannot be groomed.



LAW ENFORCEMENT

Facing incidents of online child sexual abuse and exploitation on a daily basis, law enforcement has first-hand experience of this form of crime and as such, are well placed to participate in the development and distribution of prevention and awareness raising campaigns. Raising awareness and providing children, parents, guardians and carers with the appropriate knowledge and tools are essential to reduce it.¹⁴⁶



CIVIL SOCIETY

Civil society possesses a range of expertise and information which can be an invaluable resource in reaching out or providing services to children, young people, parents, guardians and educators to help promote the online safety agenda.¹⁴⁷ Awareness raising campaigns by NGOs are often successful because of the clarity of the message, the occasion used and the support of, or collaboration with, public authorities, industry and the international community. Through awareness campaigns, advocacy organisations can influence public opinion and garner active support from the government, public, and other potential investors to help better protect children.¹⁴⁸



Commemorative days

These days provide an opportunity to draw attention to the issue, raise public awareness and apply pressure on the authorities, especially as they attract media coverage.

- ✓ The United Nations Universal Children's Day (November 20th)¹⁴⁹
- ✓ The Day of the African Child (DAC) (June 16th)¹⁵⁰
- ✓ The Safer Internet Day (SID) (in February)¹⁵¹
- ✓ The European Day on the Protection of Children against Sexual Exploitation and Sexual Abuse (November 18th)¹⁵²



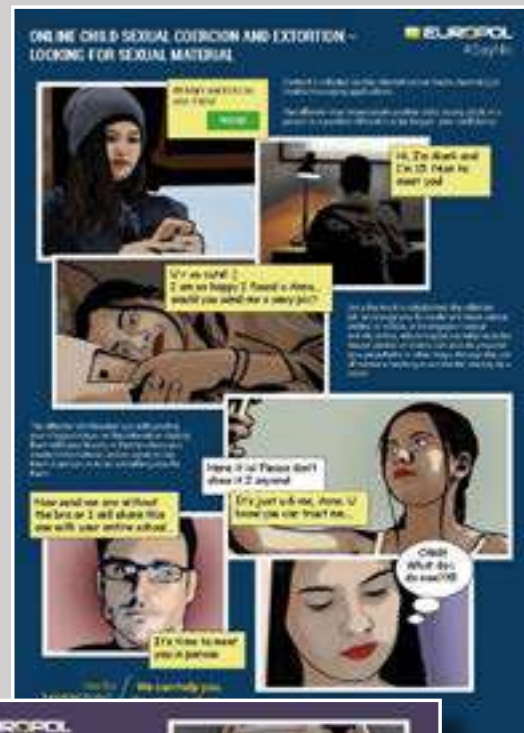
Examples of awareness-raising campaigns, launched by different actors:



NSPCC⁵⁴



ECPAT⁵³



Europol⁵⁵



4. CAPACITY BUILDING

Capacity building programmes aim to safeguard the implementation of the law and address related challenges through ensuring that professionals who are charged with enforcing the law have the knowledge and skills to carry out their duties competently.

Professionals who have regular contact with children in the sectors of health, social protection, justice and law-enforcement should have adequate knowledge on children's rights and online child sexual abuse and exploitation as well as a deep understanding of the legal provisions they are entitled to enforce.¹⁵⁶ Countries should provide training for persons involved in the proceedings as well as the treatment of victims, in particular law enforcement officers, attorneys, prosecutors, judges and child and health care personnel. The training should cover digital investigation, the preservation of evidence in IT environments and how to question children.¹⁵⁷ Training programmes should be certified to ensure quality and the level of knowledge and skills should be maintained over time. Policies should be adapted to meet changing trends and technologies to ensure the necessary resources are available for investigation of offences.¹⁵⁸



Examples of capacity building programmes



Training for law enforcement

At the international level, INTERPOL provides operational training courses that cover, among others, investigative support tools, such as forensic techniques. Furthermore, the INTERPOL Global Learning Centre (IGLC) is a web-based portal that encourages the sharing of knowledge and best practice between INTERPOL member countries as well as providing the opportunity for interactive e-learning.¹⁵⁹ At the European level, Europol holds an annual training course on “Combating the Online Sexual Exploitation of Children on the Internet” (COSEC).¹⁶⁰



Training for the judiciary

Such projects are organised, at the international level by the Cybercrime Programme Office of the Council of Europe (C-PROC),¹⁶¹ as well as at the EU level by the European Judicial Training Network (EJTN).¹⁶²



Training for social workers

The International Federation of Social Workers (IFSW)¹⁶³ is a global organisation that promotes social work, shares best practice models and facilitates international cooperation to achieve social development and social justice globally. The policy statement “Guiding Principles for Social Workers Working with Others to Identify and Protect Children From all Forms of Sexual Abuse,” grooming and CSAM included, is an example of the guidance provided by IFSW.¹⁶⁴ Benin, Kenya, Lebanon, Madagascar, Morocco, Niger, Rwanda, Tanzania and Uganda are members of the IFSW.¹⁶⁵

Moreover, the Global Social Service Workforce Alliance¹⁶⁶ provides planning, training and support (e.g. through tool kits, training material, webinars, assessments and other resources) so that social services deliver promising practices that improve the lives of vulnerable populations. Ethiopia, Ivory Coast, Kenya, Lebanon, Morocco, Rwanda, Tanzania and Uganda participate in this global network.¹⁶⁷

5. PREVENTION OF OFFENDING AND RE-OFFENDING

OFFENDER SUPPORT SYSTEMS

People with a sexual interest in children do not always want to act on their interest and harm children. On the contrary, they may be concerned and need help to keep them safe. Support systems may be addressed to people with a sexual interest in children to prevent them from offending, to offenders (convicted or not) to prevent them from re-offending, to young people with dysfunctional sexual behaviour, as well as to their family and friends. Support systems can take different forms:

Helplines

A confidential helpline or service (for example online centre) with specialist professionals that provide guidance to people with a sexual interest in children, as well as to their family and friends.



“Stop It Now!”¹⁶⁸ is an organisation that, among other services, provides direct help to individuals with questions or concerns regarding child sexual abuse.

Treatment programmes

A comprehensive therapy may be necessary for individuals with a sexual interest in children to prevent them from (re)offending. A therapeutic approach could include psychological, sexological, medical and pharmaceutical support.



The Lucy Faithfull Foundation (LFF)¹⁶⁹ in the United Kingdom works with adult male and female sexual abusers, young people with inappropriate sexual behaviour, victims of abuse and family members. It offers services such as treatment programmes to known offenders, case specific advice, training and development courses and workshops, educational programmes for internet offenders and their families, circles of support and accountability, and internet safety seminars for schools. Another example is the Prevention Network “Kein Täter Werden”¹⁷⁰ in Germany, which offers free and confidential treatment for people voluntarily seeking therapeutic help with their sexual preference for children and/or early adolescents.

MONITORING OF CHILD SEX OFFENDERS

Where the danger posed by offenders and the possible risk of repeat offences make it appropriate, convicted child sex offenders should be temporarily or permanently prevented from exercising professional activities involving direct and regular contact with children.¹⁷¹ To this end, two preventive tools should be established: screening and disqualification.

⊕ Screening

The Lanzarote Convention, in Article 5(3),¹⁷² and the Directive 2011/93/EU, in Article 10(2),¹⁷³ refer to the screening of candidates for professions that involve regular contact with children. This practice should ensure that the candidates have not been convicted of sexual offences against children. However, some countries go beyond these legal provisions, developing a more efficient screening mechanism that ensures more adequate protection of children against potential sexual abuse or exploitation, with the following characteristics:¹⁷⁴

- ✓ Mandatory screening, at least for specific activities (e.g. education, care and support of children) or with regard to more vulnerable children.
- ✓ The failure to carry out adequate mandatory screening should be made a serious criminal offence, or, in the case of legal persons, at least be subject to civil or administrative sanctions.
- ✓ Screening should comprise all types of activities involving direct and regular contact with children, regardless of whether within an employment contract or as a self-employed service provider.
- ✓ Screening should not be limited to the screening of “applicants”, at the stage of recruitment, but rather extend to regular “interval screening” during the course of the employment or assignment.

⊕ Disqualification of convicted child sex offenders

There are two systems of disqualification:

- a.** the “judiciary disqualification”, where the disqualification directly arises from the conviction as it is an additional part of the sentence delivered by the criminal court;
- b.** the “regulatory disqualification”, according to which the disqualification is linked to the conviction but it is established through a regulatory system administered by public authorities or agencies.

In addition to disqualification mechanisms, countries may use specific sex offenders registries, their main function being the monitoring of the re-insertion of convicted sex offenders after having served their prison sentence.¹⁷⁵

6. RESEARCH, DATA COLLECTION AND MONITORING

Research and data collection on online child sexual abuse and exploitation can reveal the true scope of the problem in a country. Research can identify new trends as well as strengths and weaknesses in legislation and response mechanisms. The results of such research can also inform governments and policy makers with respect to prioritising actions, developing effective strategies and tools, establishing specialised agencies and allocating the necessary human and financial resources.¹⁷⁶ Monitoring the international environment can help identify international standards and established best practice which can then be adapted to the national context. Regular monitoring and evaluation of a national action plan demonstrate whether goals have been achieved and what can be done further. Research, data collection and monitoring can be undertaken by the following actors:



NATIONAL BODY IN CHARGE OF MONITORING AND COORDINATING THE NATIONAL ACTION PLAN

The national body may undertake research and field visits to monitor the implementation of the national action plan.



INTERGOVERNMENTAL ORGANISATIONS

Intergovernmental organisations undertake research related to child sexual exploitation, collect data and monitor the implementation of their treaties in their member states.



These efforts include the UN Special Rapporteur on the sale and sexual exploitation of children,¹⁷⁷ UNICEF¹⁷⁸ and its Office of Research,¹⁷⁹ and the Council of Europe Lanzarote Committee.¹⁸⁰



CIVIL SOCIETY

Research reports and other resources on child sexual abuse and Internet safety provided by non-governmental organisations and charities across the world, coupled with information-collection from government entities, yield a better understanding of the scope of the issue and allow stakeholders to identify gaps and develop responses.¹⁸¹



ECPAT International produces global monitoring reports on the status of action against the commercial sexual exploitation of children around the world.¹⁸² ICMEC conducts research into national laws against “child pornography” in 196 countries.¹⁸³



The Family Online Safety Institute’s Global Resource and Information Directory¹⁸⁴ is a comprehensive source of peer-reviewed online safety information on a global scale. On its platform, individual country pages provide a chronicle of research, education, legislation, organisations active in the internet safety space and national response to online child sexual exploitation.



ACADEMIA

Universities and research centres with specialist knowledge of issues relating to online child sexual exploitation provide high quality research, statistics and good evidence to the public, policy makers, law enforcement and civil society. They also contribute to a better understanding of the problem and effective response at the national and international level.



The Crimes against Children Research Center (CCRC) of the University of New Hampshire in the US¹⁸⁵ and the International Centre: Researching child sexual exploitation, violence and trafficking of the University of Bedfordshire in the UK¹⁸⁶ are such examples.

7. LAW ENFORCEMENT INVESTIGATIONS

Law enforcement agencies must be able to investigate online child sexual abuse and exploitation. In addition to substantive criminal law provisions and computer forensics training, law enforcement agencies need the necessary tools and procedures to investigate so that victims of online sexual abuse or exploitation are protected and offenders apprehended. Investigatory tools and procedures must be legitimate, so that retrieved evidence is admissible in court. Efficient law enforcement investigations lead to positive judicial outcomes.¹⁸⁷

A specialised child protection unit or service, often part of the cybercrime unit, within the national law enforcement agency should be established. This unit should use child-friendly policing approaches, ensure cross-sectoral and international cooperation, and be equipped with the knowledge, skills, tools and resources necessary for handling cases of online child sexual abuse and exploitation effectively.¹⁸⁸

POLICING APPROACHES

⊕ **Child-friendly approach**

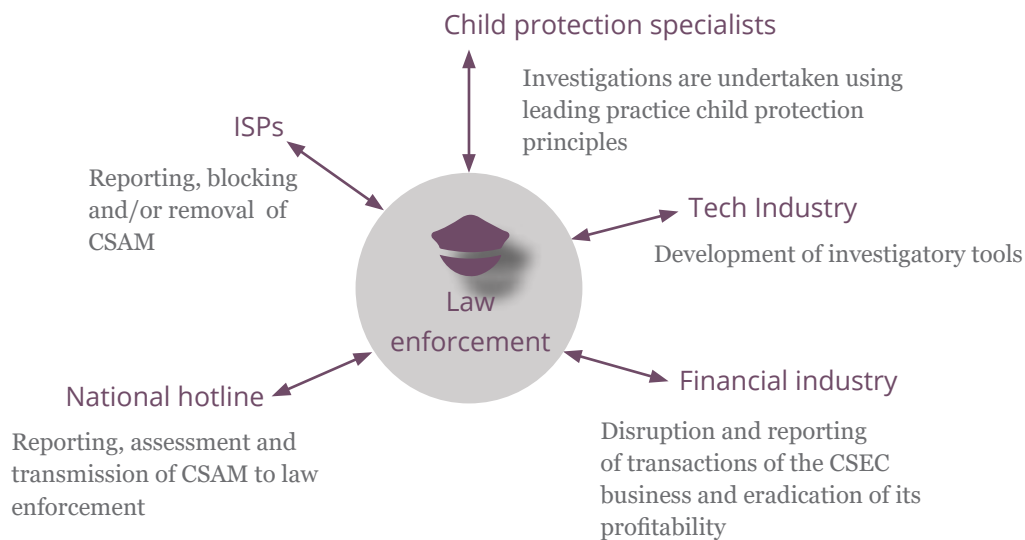
Investigations must be “*carried out in the best interest and respecting the rights of the child.*” A protective approach should be taken towards victims to prevent re-victimisation, “*ensuring that the investigations [...] do not aggravate the trauma experienced by the child.*”¹⁸⁹

⊕ **Multi-stakeholder approach**

The online sexual abuse of children cannot be combated successfully by law enforcement alone. Child protection specialists and NGOs are involved in investigations to ensure that they are undertaken using leading practice child protection principles.¹⁹⁰ The tech industry builds investigatory tools that are used by law enforcement,¹⁹¹ while the financial industry, in conjunction with law enforcement, disrupts the economics of the CSEC business and eradicates its profitability.¹⁹² To facilitate reports of child sexual abuse material, law enforcement cooperate with national hotlines.¹⁹³ Finally, law enforcement engages with online service providers, which establish reporting mechanisms in the very environments in which a child or young person may be subject to unwanted contact, or in which child abuse imagery may be discovered; mechanisms that warn potential offenders that law enforcement is present within a specific environment.¹⁹⁴



The Child Exploitation and Online Protection command (CEOP) in UK is an example of a law enforcement agency which employs such holistic approach.¹⁹⁵



✦ International approach

Given the international nature of online child sexual abuse, effective cooperation in law enforcement at the international level is imperative in order to address the problem on a global scale. With dedicated law enforcement officers who have the required knowledge, skills, systems and tools, a country will be able to lead and coordinate complex child sexual abuse and exploitation investigations and liaise effectively with international law enforcement to advance investigations that cross borders.¹⁹⁶



INTERPOL facilitates communication and cooperation between members of the international police community,¹⁹⁷ and, in the field of online child sexual abuse and exploitation, assists its member states with special tools and services.¹⁹⁸ International law enforcement cooperation is also supported by the Virtual Global Taskforce (VGT),¹⁹⁹ an international alliance of law enforcement agencies²⁰⁰ and private sector partners²⁰¹ working together to combat online child sexual exploitation and other forms of transnational child sexual exploitation. At the EU level, Europol's European Cybercrime Centre (EC3)²⁰² supports the competent authorities in Member States in preventing and detecting all forms of criminality associated with the sexual exploitation of children.²⁰³ At the African level, the African Union established, in February 2014, the African Mechanism for Police Cooperation (AFRIPOL),²⁰⁴ in its role to enhance inter-state police cooperation, particularly in addressing transnational crime. AFRIPOL became operational in April 2016.²⁰⁵



In May 2014, an international operation, coordinated by INTERPOL, targeting organised crime networks behind sexual extortion cases around the world, had resulted in the arrest of 58 individuals. Close cooperation of the international law enforcement community led to the identification of between 190 and 195 individuals working for organised crime groups operating from the Philippines and to the identification of sexual extortion victims in Indonesia, the Philippines, Singapore, the United Kingdom and the United States. Potential victims were also traced to Australia, South Korea and Malaysia in addition to the hundreds of individuals in Hong Kong and Singapore already reported as victims.²⁰⁶

INVESTIGATORY TOOLS

✦ Victim identification

Victim identification²⁰⁷ is the analysis of child abuse material with the objective of locating the child and/or abuser portrayed. It is a victim-centric approach to investigation, which emerged in recent decades out of a clear need to act upon child abuse material found circulating online and seized by the police from computers and other storage devices. Online victim identification combines image analysis and traditional investigative methods. Child abuse material is more likely to show the face of the victims than the abuser. And since the abuser is most often a person known to the child, such as a parent, uncle, neighbour or childcare professional, by identifying and locating the child, the child's abuser can also be identified and brought to justice.²⁰⁸



The International Child Sexual Exploitation (ICSE) image database, managed by INTERPOL, is an intelligence and investigative tool: a central database which allows victim identification specialists to share data with colleagues across the world. As of January 2017, 10,000 victims of child abuse had been identified and rescued.²⁰⁹ Currently 49 countries are connected to the ICSE database.²¹⁰ Furthermore, Project VIC²¹¹ uses hash matching technology²¹² to create a “fingerprint” that can be used to identify a unique image or video and helps law enforcement to distinguish child sexual material which is already known from that which is unknown. This prevents copies of known material from having to be investigated again and enables detectives to focus on new material that might involve children who have yet to be identified. More than 2,500 law enforcement agencies in 40 countries use the technology developed by Project VIC's partners to rescue child victims, apprehend offenders and secure crime scenes.



An operation into the exchange of child sexual abuse material via the messaging application WhatsApp led to 38 arrests in Latin America and Europe (Argentina, Bolivia, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Germany, Guatemala, Italy, Mexico, Paraguay, Peru, Portugal and Spain). The codenamed “Operation Tantalio” was launched in 2016 by the Spanish National Police and coordinated by INTERPOL and Europol. Hundreds of images and videos discovered were shared with INTERPOL and Europol via the ICSE database.²¹³

✦ Reporting platform

Within the national law enforcement agency, the specialised unit for cybercrime or online child sexual abuse and exploitation acts as a single entry point for reports of child sexual abuse material or inappropriate sexual behaviour on the Internet. This platform centralises all reports received from the public, industry, child protection services, national helplines and hotlines, and international law enforcement. As a single point of entry, this platform ensures that all reports are recorded, risk assessed and prioritised in a consistent, coordinated, efficient and effective manner.²¹⁴ Monitoring the number of reports and the type of offences reported over the years, the reporting platform could enable the statistical analysis of online child sexual exploitation, and prove a useful tool for policy makers.



The French reporting platform PHAROS²¹⁵ (French acronym for Reports Harmonization, Analysis, Cross-checking and Orientation Platform) is an example of such a platform.²¹⁶

✦ Undercover operations

An undercover operation is an investigatory technique that allows police officers to use a concealed identity while conducting investigations online.²¹⁷ Acting as either children on the Internet or offenders seeking other child sex offenders online, undercover (sting) operations allow law enforcement agents to detect and infiltrate their networks, with the aim of preventing further child sexual abuse and exploitation from being committed. Undercover operations may aid prosecutions and deterrence by providing credible, direct evidence as law enforcement may catch offenders in the act. This evidence reduces the need for innocent parties or victims to testify and become involved in the judicial process, which in turn reduces the risk of re-victimisation and prevents further traumatisation.²¹⁸ Therefore, in order to combat online sexual exploitation of children efficiently, undercover operations should be allowed under national legal frameworks.



Undercover operations have been carried out in Bosnia Herzegovina, Bulgaria, Italy, Portugal, Serbia, Sweden, Switzerland, United Kingdom, United States,²¹⁹ Poland,²²⁰ France,²²¹ Greece,²²² often with the appropriate authorisations and as long as the investigator does not induce or instigate the commitment of a crime.

8. REPORTING ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION

REPORTING MECHANISM

Reporting mechanisms, such as a hotline or reporting portal, enabling the public to report suspected or actual cases of online child sexual abuse or exploitation should be developed in order for law enforcement to be informed and to launch an investigation. Online child sexual abuse and exploitation can occur in many ways and places, including through websites, emails with links to inappropriate content, peer-to-peer (P2P) file sharing networks, newsgroups, instant messaging or online gaming. The person reporting the abuse will need to provide different types of information depending on the features of the reporting platform: date and time, URL, email address, IP address, chat service or game console and group name.

Reporting mechanisms may be managed by entities which could include a government agency, child protection services, an NGO or a recognised self-regulatory organisation.²²³ These entities with the legal competency to receive such reports assess them according to strict criteria and transmit content considered illegal to the relevant law enforcement agency for further investigation and victim identification as well as, in many cases, to the ISP²²⁴ hosting the content for blocking and/or removal.

Ideally, such mechanisms should provide the possibility to report anonymously and combine advice with support in order to encourage victims and their families to report incidents of abuse, which would otherwise remain hidden because of the fear of stigmatisation or the lack of trust in available public services.²²⁵

These mechanisms should be available nationwide, 24 hours a day and 7 days a week, free of charge, easily accessible to children and adults, staffed by properly trained personnel and sustainable, regardless of current technology and available resources.²²⁶

Additionally, the Internet industry could provide links to national hotlines from their websites,²²⁷ promoting reporting mechanisms for child sexual abuse material and making sure that customers know how to report such material.

National legislation should provide for the establishment of a hotline or reporting portal. In addition, the framework of cooperation between the reporting mechanism and the law enforcement agency and between the reporting mechanism and ISPs should be formally agreed.²²⁸



A national hotline can become a member of the International Association of Internet Hotlines (INHOPE),²²⁹ a collaborative global network of hotlines dealing with illegal content online and committed, together with its industry and law enforcement partners, to stamping out child sexual abuse on the Internet. INHOPE helps the development of new hotlines worldwide, while supporting and sharing knowledge with its members. INHOPE's members follow common procedures for receiving and processing reports in compliance with a set of best practice.²³⁰ The Internet Watch Foundation (IWF)²³¹ in the UK, Point de Contact²³² in France, the CyberTipline²³³ in the US, the CyberReport Hotline - Office of the Children's eSafety Commissioner²³⁴ in Australia and the Safer Internet Association (SIA) Japan²³⁵ are some of the 54 INHOPE members in 45 countries worldwide.²³⁶ The African continent has only one INHOPE member, in South Africa, established by the Film and Publication Board,²³⁷ while Uganda uses the IWF Portal.²³⁸

Arda Gerkens, INHOPE President and Managing Director of the Dutch hotline, Interview 15/02/2017.

“The more widespread access to the Internet becomes, the more victims there will be. If we don't start addressing this issue now in Africa, it will be too late. The problem is not whether or not the material is hosted in African countries but the fact that the material is online and therefore accessible. Whoever surfs the internet and searches for pornography may come across child sexual abuse material. So there must be a way to report it. The material doesn't have to be produced or hosted in Africa. As long as it is viewed in Africa, you need a reporting mechanism where the report can be made in the local language(s). The reporting mechanism or hotline can then verify whether the material is hosted in its own country or in another country, the Netherlands for example. If the material is hosted in the Netherlands, they can report it to us via INHOPE.”

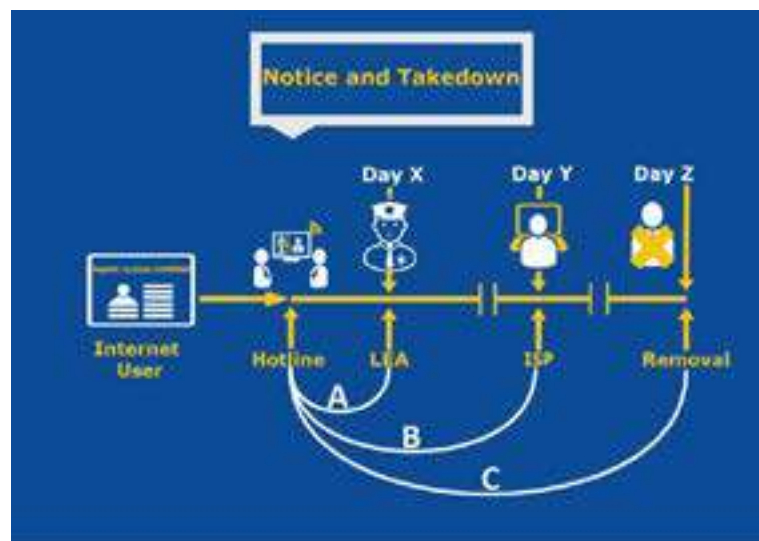


A report made to the US National Center for Missing and Exploited Children (NCMEC) via its CyberTipline, followed by swift international police cooperation led to the arrest on 24 February 2015 of a Romanian man suspected of sexually abusing his two-year-old daughter and then posting images of the abuse online. The NCMEC transmitted the information to US Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and Europol who immediately launched an investigation and liaised with Romanian law enforcement authorities to ensure the identification and safeguarding of the victim.²³⁹

REMOVAL AND BLOCKING OF CHILD ABUSE CONTENT

⊕ Notice and Takedown procedure

“Notice and takedown” is considered a vital tool in removing CSAM at its source, keeping the Internet free of this content, and disrupting the cycle of sexual exploitation and abuse of children and their re-victimisation. It refers to a company’s procedures for handling 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.²⁴⁰ ISPs remove (“takedown”) the illegal content, as soon as they have been made aware (“notice”) of its presence on their services.²⁴¹ When CSAM is hosted in the country, it must be removed promptly, reducing its volume on the Internet. When CSAM is hosted outside of country, and until its removal at the source, blocking access towards internet users could be a temporary solution, disrupting offenders’ access to it and further distribution.²⁴² Apart from statutory regulated notice and takedown procedures, ISPs and others in the industry may also take voluntary action to prevent the misuse of their services by explicitly forbidding child sexual abuse material in their terms and conditions and by removing it from their services.²⁴³



Most common Notice and Takedown process²⁴⁴

⊕ National list of websites containing CSAM

“Both with a view to the removal and the blocking of child abuse content, cooperation between public authorities should be established and strengthened, particularly in the interests of ensuring that national lists of websites containing child pornography material are as complete as possible and of avoiding duplication of work.”²⁴⁵ Use of this national list of websites provided by the national police and whose distribution is illegal according to national legislation, is the best option for (Internet) Access Service Providers (ASPs) wishing to block access to child sexual abuse material. For ASPs in countries where this is not possible, INTERPOL offers the “Worst of” list of domains,²⁴⁶ containing the most severe known child sexual abuse material.

In the event of blocking access to child sexual abuse material, Internet traffic is redirected to a “stop page”, hosted on an ASP server. The page provides a complaints mechanism as well as links to further information related to CSAM and its distribution on the Internet.



MANDATORY REPORTING

Any person who knows of or suspects the sexual abuse or exploitation of a child should report it to law enforcement authorities and/or to a national hotline.²⁴⁷ However, reporting CSAM should be a clear legal obligation for certain individuals and organisations:²⁴⁸

⊕ Professionals

Confidentiality rules imposed by national legislation on certain professionals who work with children (healthcare professionals, social services, teachers, law enforcement) should not apply for cases of child sexual abuse or exploitation. These professionals should report any situation where they have reasonable grounds for believing that a child is the victim of sexual abuse or exploitation.²⁴⁹ Likewise, reporting should be mandatory for individuals who, in their everyday, professional capacity, do not come into contact with children, but might potentially be exposed to CSAM as a result of their profession, such as computer technicians and photo developers. They may come across evidence of CSAM while repairing or servicing a computer, monitoring social networking websites or apps, accessing links or pop-ups, or using image-hosting or file-sharing software. This class of professionals should not be required to search for the illegal material, but rather to report it to the appropriate authorities if discovered.

⊕ ICT and financial industry

Given the heavy traffic in CSAM over the Internet, ISPs are in an ideal position to report suspected online child sexual abuse and exploitation to law enforcement through content management and reports from their users. Legislation should provide companies with the authority and confidence to process this material,²⁵⁰ including the Notice-and-Takedown procedure, while guidance and training should be provided to staff for the safe handling and transmission of illegal content. As a result, the Internet industry keeps their services clean and safe, protects its customers, especially younger users, and helps to deter offenders.

9. ASSISTANCE AND PROTECTION MEASURES FOR VICTIMS

ASSISTANCE TO VICTIMS

Children who are victims of sexual abuse and/or exploitation, either offline or online, may not recognise themselves as victims and remain in a state of denial. They may not receive proper support from their families, who may not know how to help their children or may remain unaware of the situation. Victims often become more vulnerable and susceptible to depression, self-harm or suicide caused by feelings of isolation.²⁵¹ Therefore, victims and their parents or guardians, should receive advice and assistance immediately.²⁵² They should continue to receive support throughout the investigation and legal proceedings to reduce additional trauma, and for as long as necessary for the child's physical and psychological recovery, which may take many years. Assistance to victims include:

⊕ **Child helplines**

Children need to know that they are not alone. If they do not feel comfortable speaking with a family member, a friend or statutory services, it is important that they can turn to an anonymous, confidential support service. Helplines can be accessed via a variety of means, such as telephone, email, text messaging, internet chat services/internet messaging, discussion forums, email and face-to-face meetings, and are ideally confidential, anonymous and accessible free of charge, 24 hours a day and 7 days a week. Helplines are run by civil society organisations or government agencies and operate in partnership with key referral services, working closely with educational facilities, hospitals, law enforcement, judicial services, shelters, and other child-related services.²⁵³



Helplines within the Insafe network of Safer Internet Centres (SICs)²⁵⁴ provide information, advice and assistance to children, young people and parents on how to deal with harmful content, harmful contact such as grooming, and harmful conduct such as sexting. Child Helpline International²⁵⁵ supports the creation and strengthening of national toll-free child helplines worldwide, and uses child helpline data and knowledge to highlight gaps in child protection systems and advocate for the rights of children. This global network consists of 181 child helplines and other organisations operating in 139 countries around the world.

⊕ Individual needs assessment

Assistance provided to victims should reflect an assessment of the circumstances particular to the child in question. The purpose of an individual needs assessment²⁵⁶ is to define which special support measures are in the best interests of the child. It implies an integrated and multidisciplinary approach between social services, law enforcement and medical professionals who assess the victim's status and draw up an individual welfare plan according to her/his needs.²⁵⁷ As the needs of victims may change over the time, it is also necessary to review the welfare plan periodically.

Children's houses or child protection centres, with such multidisciplinary approach, are particularly well placed to conduct individual needs assessment of child victims.²⁵⁸



The “Barnahus” model

Addressing child sexual abuse and exploitation is not only a judicial issue but requires comprehensive and multiagency intervention. The Barnahus²⁵⁹ (which literally means Children's House), established in Iceland in 1998, is a child-friendly, interdisciplinary and multiagency centre whereby different professionals work under one roof to investigate suspected cases of child sexual abuse and to provide appropriate support for victims thereby improving cooperation between the different stakeholders and reducing the trauma for the victim and her/his family. The Barnahus model has been adapted and implemented in a number of other countries. Agencies in Sweden, Norway and Denmark have all tailored the model to their particular social, legal and political context.²⁶⁰ The model is recommended as good practice by the Council of Europe.²⁶¹

CHILD-FRIENDLY JUSTICE

Children can come into contact with the justice system for a variety of reasons: family matters such as divorce or adoption; administrative reasons such as nationality or immigration issues; or as victims, witnesses or perpetrators of crimes. Naturally, they feel vulnerable as they are thrown into an intimidating adult world that they cannot understand. They become even more vulnerable when faced with the justice system as victims of sexual abuse and/or exploitation. Therefore, they require a high level of support to be able to participate effectively in the judicial process, which should not cause them additional trauma, and to maintain their engagement throughout.²⁶² Adapting justice to their needs is necessary. As the CRC, Article 3(1) sets forth, “[i]n all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interest of the child shall be a primary consideration.”

Measures during criminal proceedings include:²⁶³

- ✓ Judiciary and prosecutors with specialist knowledge and skills for handling CSA/CSE cases, who take into consideration the potential vulnerability of child victims/witnesses and the methodologies and profiles of the offenders, enabling positive judicial outcomes for the victims.²⁶⁴
- ✓ The explanation of proceedings to victims in age-appropriate language.
- ✓ The involvement of the parents or guardians, where possible and appropriate.
- ✓ The provision of effective support, including emotional and psychological support, to child victims and witnesses by specialists.
- ✓ The appointment of a special representative for child victims, where there is a conflict of interest between the child victim and the holders of parental responsibility or where the child is unaccompanied or separated from the family.
- ✓ Access to legal counselling and to legal representation, including for the purpose of claiming compensation, which should be free of charge where the victim does not have sufficient financial resources.
- ✓ Interviews with child victims take place in premises designed or adapted for this purpose²⁶⁵ and are carried out by trained officials (police officers and judges) or through specialised professionals (psychiatrists or psychologists) that are invited to assist. Interviews are carried out by the same persons and their number is as limited as possible. Repetitive and unstructured interviews can distort the child’s account and cause additional trauma. Legislation should allow for interviews to be audio-visually recorded and the recordings to be used as evidence in criminal court proceedings.
- ✓ During criminal court proceedings, the child is heard without the presence of the public or without being present her/himself through the use of appropriate communication technologies.

Guidelines on child-friendly justice are provided by the United Nations,²⁶⁶ and the Council of Europe.²⁶⁷



10. INDUSTRY ENGAGEMENT

Companies that develop, provide or make use of information and communication technologies in the delivery of their products and services have a responsibility to promote the online safety of children and to address the issue of online child sexual abuse and exploitation.

POLICIES AND PROCEDURES

All providers and sources of Internet access need to be involved: computers, mobile operators, ISPs, social networks, gaming and file sharing platforms, e-mail providers and search engines as well as cybercafés (which is where children in some African countries are most likely to access the Internet). In order for companies to identify, report and remove child sexual abuse material, as well as to prevent their platforms from being used for child sexual exploitation, they should take the following measures:²⁶⁸

⊕ Preventing child safety online

- ✓ A child safeguarding policy is developed or risks relating to child protection are integrated into companywide policy commitments.
- ✓ Terms of use and codes of conduct explicitly prohibit customers to use company services/ platforms for the purposes of child sexual abuse and exploitation or the production, distribution or viewing of CSAM and inform that such content will be removed and reported.
- ✓ Clear rules are communicated in accessible and easily understood language that emphasises what behaviour is and is not acceptable, informs how to use reporting mechanisms, describes safety settings, and is particularly geared for young users and for their parents and caregivers.
- ✓ Underage access and exposure to inappropriate content or services are prevented by providing appropriate technical measures, such as parental control tools, block/allow lists, and content filtering.
- ✓ Where national legislation is not yet at international standards, companies bring their business practices in line with those standards on a voluntary basis.²⁶⁹
- ✓ Written procedures ensure the consistent implementation of policies that protect freedom of expression and privacy for all users, including children, as well as the documentation of compliance with these policies.
- ✓ Collaborative action and information sharing regarding threats, intelligence, knowledge and best practice within specific sectors, as well as with law enforcement, civil society and other industry partners.

⊕ Reporting and removal of CSAM

- ✓ A specific individual and/or a team is designated with responsibility for processing CSAM and has access to the necessary internal and external stakeholders.
- ✓ A reporting mechanism allows users to report CSAM or inappropriate contact as well as its specific profile/location.
- ✓ A notice and takedown procedure is in place.
- ✓ Image/video photo hash systems are in place to screen images/videos proactively against a known set of illegal child sexual abuse images/videos and to remove/report them.
- ✓ Lists of websites containing CSAM are used to identify and remove links that host known CSAM.
- ✓ Partnerships with law enforcement and hotlines are established to promote reporting of CSAM and to strengthen cooperation in relevant investigations.

⊕ Measures appropriate for specific sectors

Social networks: Algorithms flag users over a certain age who befriend numerous underage individuals, or who send messages to multiple strangers. Additionally, monitoring age and name changes ensures that users are not falsely representing themselves. Settings should protect children's privacy through preventing their photos from appearing in public search results and through preventing them from accidentally sharing their location, photos, or other information enabling people outside their networks to identify them.

Online payment services: Transactions with prepaid credit cards should be limited, as this allows consumers to remain anonymous thereby hampering the identification of potential perpetrators.

Cybercafés: Codes of conduct are developed. It should be mandatory for users to provide their credentials before using cybercafé facilities, to ensure that they can be traced if they commit any illicit activity while on the Internet as well as to deter inappropriate behaviour online. Moreover, children should not use the same computers as adults in order to reduce the risk of them being accidentally exposed to age-inappropriate content (from the browser history, chat logs, downloaded files etc.).²⁷⁰ Filters should also be installed to block age-inappropriate content.

DEVELOPING INNOVATIVE SOLUTIONS

Technology companies are well placed to drive innovation in the fight against online child sexual abuse and exploitation. They are in a position to anticipate technological developments and to identify new and emerging online trends and patterns that could be exploited by child sex offenders.²⁷¹



Examples of innovative solutions development:

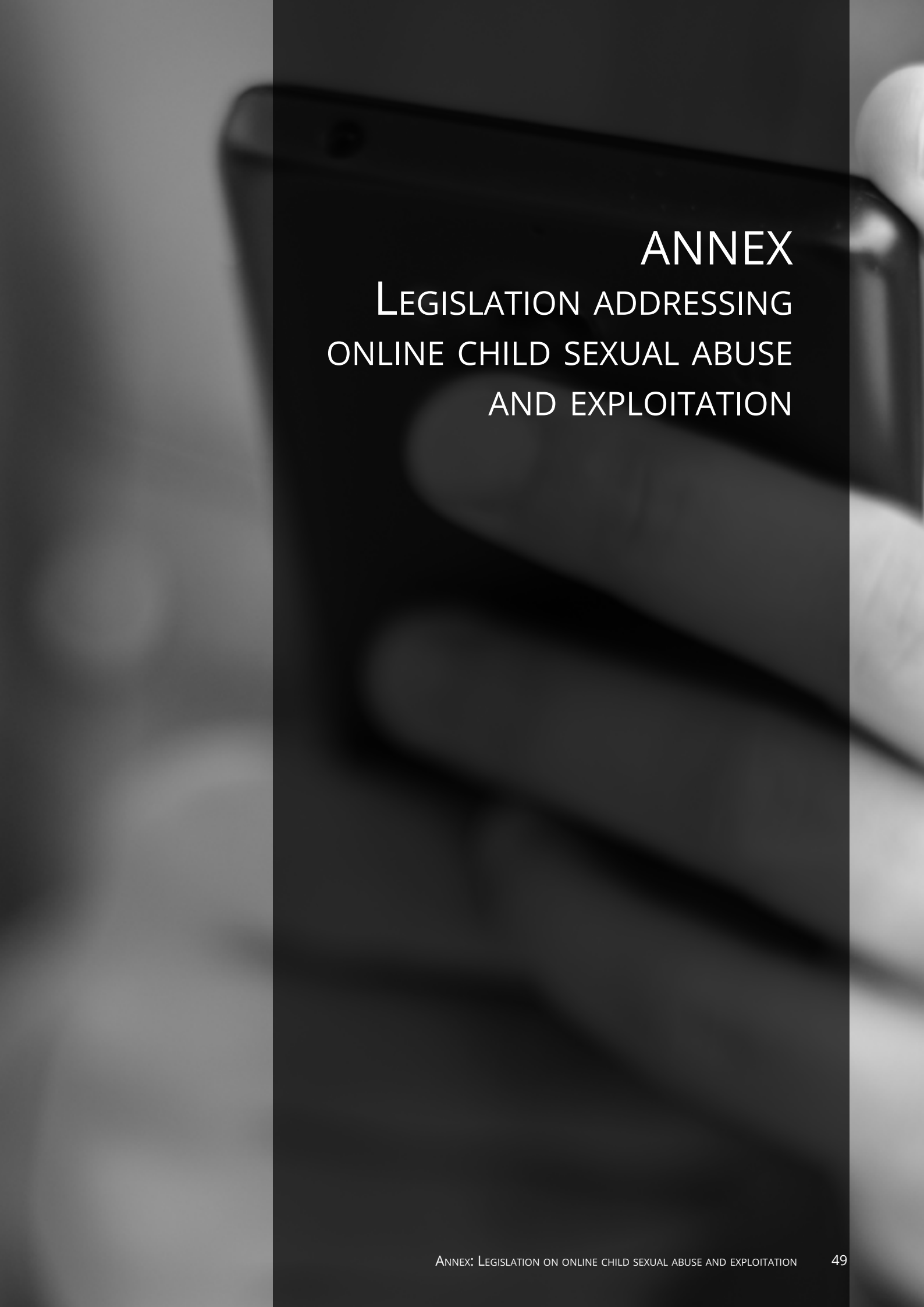
- ✓ PhotoDNA,²⁷² developed by Microsoft, is a technology that enables the identification of known images of child sexual abuse through hash comparison and matching.
- ✓ Spotlight,²⁷³ developed by Thorn,²⁷⁴ is a tool that helps law enforcement identify victims of sex trafficking more rapidly.
- ✓ Industry Hash Sharing Platform,²⁷⁵ developed by Thorn in collaboration with Facebook, Google and other technology industry leaders, is a cloud-based hash sharing tool, and the first collaborative industry initiative to improve and accelerate the identification, removal and reporting of child abuse images across different digital networks.
- ✓ NetClean²⁷⁶ develops technological solutions for combating child sexual abuse material. NetClean's sister company, Griffeye, provides law enforcement worldwide with an intelligence and visual big data platform for collecting, processing, analysing, visualising and managing CSAM, the Griffeye Analyze Platform.²⁷⁷



The Technology Coalition,²⁷⁸ powered by leaders in the Internet services sector, supports the development of technology solutions that disrupt the ability to use the Internet to exploit children sexually and to distribute child sexual abuse material, including reporting processes and procedures. It also seeks and creates platforms for collaboration with the private and public sectors for the creation of standards and the sharing of best practice. With regard to the financial industry, credit cards, money transfers, digital currency, and other payment methods are used to purchase or to obtain access to CSAM. Financial companies must be vigilant and should be required to report these transactions to law enforcement or another mandated agency.



The Financial Coalition Against Child Pornography (FCACP)²⁷⁹ is a cooperative initiative between the financial and Internet industries to help eradicate the proliferation of commercial child pornography, one of its chapters being to prevent child pornography merchants from entering the payments system and establishing merchant accounts with members of the FCACP.



ANNEX
LEGISLATION ADDRESSING
ONLINE CHILD SEXUAL ABUSE
AND EXPLOITATION

1. INTERNATIONAL AND REGIONAL LEGAL FRAMEWORK

Online child sexual abuse and exploitation is a global problem that demands a global response. National jurisdictions often differ in terms of what constitutes a sexual offence, the level of law enforcement and how crimes are investigated as well as the severity of sentences and assistance available to the victims. These factors can encourage sexual predators to travel to countries with weaker legislation in order to abuse children with impunity. Furthermore, as the Internet has no borders it can also enable child sex offenders to abuse children in other countries. **It is therefore essential to harmonise national legislations and to strengthen cooperation between countries in order to improve the protection of children against such crimes.**

Online child sexual abuse and exploitation are addressed by numerous international and regional treaties, which approach the issue either from a child rights perspective or from the perspective of cybercrime prevention. This demonstrates the passage of child sexual abuse and exploitation from the offline to the online world and the impact of ICTs on children's lives as well as child protection issues. However, these instruments are sometimes incomplete because certain forms of online child sexual abuse and exploitation did not exist at the time of their drafting, or because they focus on a regional context. Nevertheless, they complement each other and represent significant progress in combating online child

sexual abuse and exploitation. As a result, countries should make efforts to transpose international and regional legal instruments into national legislation and to strengthen global cooperation.

UNITED NATIONS CONVENTION ON THE RIGHTS OF THE CHILD, 1989

The Convention on the Rights of the Child (CRC)²⁸⁰ is the first legally binding international instrument to incorporate the full range of human rights for children – including civil, cultural, economic, political and social rights –²⁸¹ and the most widely ratified human rights treaty in the world.²⁸² The CRC aims to ensure that children are safeguarded against all forms of abuse and exploitation, addressing sexual abuse and exploitation specifically in Article 34, which sets forth that, “[s]tates [p]arties 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.”

Currently, 196 countries are party to the Convention, including every member of the United Nations except the United States of America.²⁸³

The Committee on the Rights of the Child is the body of 18 independent experts responsible for monitoring implementation of the CRC by its State parties.²⁸⁴ Furthermore, in 1990, the United Nations Commission on Human Rights created the UN Special Rapporteur on the sale and sexual exploitation of children.²⁸⁵ The Special Rapporteur is mandated²⁸⁶ to analyse the root causes of the sale and sexual exploitation of children, to identify new trends and patterns, to exchange good practice for combating the problem, to promote measures for prevention, and to make recommendations for the rehabilitation of its victims. The Special Rapporteur has four main activities, namely undertaking country visits,²⁸⁷ sending individual complaints, writing thematic reports and conducting awareness-raising and advocacy to promote and protect child rights. The recommendations of the Special Rapporteur primarily target governments, UN bodies, the business sector and non-governmental organisations.

AFRICAN CHARTER ON THE RIGHTS AND WELFARE OF THE CHILD, 1990

The African Charter on the Rights and Welfare of the Child (ACRWC)²⁸⁸ is a region-specific child rights instrument. While building on the same basic principles as the UN Convention on the Rights of the Child, the ACRWC highlights issues of special importance in the African context,²⁸⁹ prohibiting, for example, child marriage and betrothal²⁹⁰ and the use of children as beggars,²⁹¹ granting girls the right to return to school after pregnancy²⁹² and tackling specific African issues that affect children, such as regimes practicing ethnic, religious or other forms of discrimination.²⁹³ Article 1(3) sets forth that “[a]ny custom, tradition, cultural or religious practice that is inconsistent with the rights, duties and obligations contained in the present Charter shall to the extent of such inconsistency be discouraged.”²⁹⁴

Specific provision on child sexual abuse and exploitation exists in Article 27, which sets forth that: “*State Parties to the present Charter shall undertake to protect the child from all forms of sexual exploitation and sexual abuse and shall in particular take measures to prevent: (a) the inducement, coercion or encouragement of a child to engage in any sexual activity; (b) the use of children in prostitution or other sexual practices; (c) the use of children in pornographic activities, performances and materials.*”

To date, the ACRWC has been ratified by 48 of the 55²⁹⁵ states of the African Union, and signed but not ratified by the remaining seven states.²⁹⁶ The African Committee of Experts on the Rights and Welfare of the Child (ACERWC) is mandated to promote and protect the rights and welfare of the child.²⁹⁷ As such, the Committee monitors implementation of the Charter and ensures protection of children’s rights²⁹⁸ by examining reports submitted by

State Parties. States are supposed to submit an initial report within two years of ratification of the ACRWC and every three years thereafter.²⁹⁹

INTERNATIONAL LABOUR ORGANISATION CONVENTION 182 CONCERNING THE PROHIBITION AND IMMEDIATE ACTION FOR THE ELIMINATION OF THE WORST FORMS OF CHILD LABOUR, 1999

The ILO Convention 182 concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (ILO C182),³⁰⁰ also named Worst Forms of Child Labour Convention, calls for the prohibition and the elimination of the worst forms of child labour, as a matter of urgency. The Convention includes in the worst forms of child labour, among others, all activities which sexually exploit children,³⁰¹ specifying in Article 3(b) *“the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances”*.

To date, the ILO C182 has been ratified by 180 out of 187 ILO member states.³⁰²

OPTIONAL PROTOCOL TO THE CONVENTION ON THE RIGHTS OF THE CHILD ON THE SALE OF CHILDREN, CHILD PROSTITUTION AND CHILD PORNOGRAPHY, 2000

The Optional Protocol on the sale of children, child prostitution and child pornography (OPSC or Optional Protocol)³⁰³ supplements the CRC by providing States with detailed requirements to end the sexual exploitation and abuse of children. States that have ratified the OPSC also commit to protecting children from being sold for non-sexual purposes such as forced labour, illegal adoption and organ donation.

It is primarily a juridical tool aimed at defining and prohibiting children’s involvement in prostitution and pornography.³⁰⁴ Specific to child sexual exploitation and child pornography:

- Article 2(c) defines “child pornography” as “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.”
- Article 3(1) requires State Parties to criminalise child sexual exploitation and child pornography, whether “committed domestically or transnationally or on an individual or organized basis.”
- Article 3(1)(c) requires State Parties to criminalise the production, distribution, dissemination, import, export, offer, sale or simple possession of child pornography.
- Article 3(4) addresses the liability of legal persons and encourages each State Party to establish such liability for offences specific to child pornography.

- Article 10(1) addresses the need for international cooperation.³⁰⁵

The OPSC has been ratified by 173 countries.³⁰⁶

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, 2001

The Council of Europe Convention on Cybercrime,³⁰⁷ also known as the Budapest Convention, is the first international treaty on crimes committed via the Internet and other computer networks, aiming principally at (i) harmonising the domestic criminal substantive legal elements of offences and connected provisions in the area of cyber-crime; (ii) providing criminal justice authorities with procedural powers to secure electronic evidence in relation to any crime; and (iii) engaging in efficient international cooperation.³⁰⁸

The Convention deals specifically with offences related to child pornography in Article 9. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography, thereby modernising legal provisions that had previously criminalised only traditional forms of the production and physical distribution of child pornography. It was felt that, *“with the ever-increasing use of the Internet as the primary instrument for trading such material, [...] specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children.”*³⁰⁹

Article 9(1) requires Member States to establish as criminal offences under their domestic law the production of child pornography for the purpose of its distribution through a computer system; offering or making available

child pornography through a computer system; the distribution or transmission of child pornography through a computer system; procuring child pornography through a computer system for oneself or for another person; and the possession of child pornography in a computer system on a computer-data storage medium. Article 9(2) defines “child pornography” as pornographic material that visually depicts either a minor engaged in sexually explicit conduct; or a person appearing to be a minor engaged in sexually explicit conduct; or realistic images representing a minor engaged in sexually explicit conduct.

Furthermore, Article 11 criminalises aiding or abetting the commission of all the offences related to child pornography as well as the attempt to distribute or transmit child pornography, or to produce child pornography for the purpose of its distribution through a computer system. Article 12 addresses the liability of legal persons while Article 23 addresses the issue of international cooperation. Finally, because of the serious nature of these offences, Article 13 demands *“effective, proportionate and dissuasive sanctions, which include deprivation of liberty in case of natural person”*, and *“effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions”*, in case of legal persons.

The Budapest Convention is open for signature by the member States and the non-member States that participated in its elaboration and for accession by other non-member States.³¹⁰ As a result, it is the most widely used multilateral instrument for the development of cybercrime legislation.³¹¹ Indeed, at present 55 countries (43 member States and 12 non-member States) have ratified the Convention and 4 countries (3 member States and 1 non-member state) have signed, but not ratified it.³¹²

“ C-PROC advises African countries *“to follow the Budapest Convention from the outset when preparing domestic legislation. This would then also facilitate accession to the Budapest Convention without further amendments should a country wish to do so. African States will need to cooperate with the authorities of countries in other regions of the world where electronic evidence is often stored or where service providers are located. The most relevant States in this respect are already Parties to the Budapest Convention. Joining this treaty would offer a legal framework for African countries to engage in cooperation with these countries.”*³¹³ ”

The Cybercrime Programme Office of the Council of Europe (C-PROC)³¹⁴ assists countries worldwide in strengthening the capacity of their legal systems to respond to the challenges posed by cybercrime and electronic evidence based on the standards set by the Budapest Convention. This includes support for strengthening legislation on cybercrime and electronic evidence in line with rule of law and human rights; training judges, prosecutors and law enforcement officers; establishing specialised cybercrime and forensic units and improving interagency cooperation; promoting public/private cooperation; enhancing the effectiveness of international cooperation; and protecting children against sexual violence online.

The GLACY+ project (Global Action on Cybercrime Extended)³¹⁵ supports seven countries in Africa and the Asia-Pacific region – Mauritius, Morocco, Senegal, South Africa, Sri Lanka and Tonga. An example of this support is the first Regional Introductory Judicial Training of Trainers (ToT) on Cybercrime and Electronic Evidence that took place on 14-17 March 2017 in Dakar, Senegal. A group of 30 magistrates (judges and prosecutors) and other judicial officers from 10 countries in West Africa including Benin, Burkina Faso, Ivory Coast, Mali, Niger and Togo, took part in the training.³¹⁶

COUNCIL OF EUROPE CONVENTION ON THE PROTECTION OF CHILDREN AGAINST SEXUAL EXPLOITATION AND SEXUAL ABUSE, 2007

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,³¹⁷ also known as the Lanzarote Convention, is the most comprehensive international legal instrument on the protection of children against sexual exploitation and sexual abuse. It focuses on ensuring the best interests of children through prevention of abuse and exploitation, protection and assistance for victims, punishment of perpetrators, and promotion of national and international law enforcement cooperation.³¹⁸

The Lanzarote Convention specifically criminalises online child sexual abuse and exploitation.³¹⁹ Article 20(2) defines child pornography as *“any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes.”* Article 20(1) criminalises the production, offering, distribution, possession and online viewing (*“knowingly obtaining access, through information and communication technologies”*) of child sexual abuse and exploitation material. The solicitation of children for sexual purposes, including online and offline grooming, is also a criminal offence according to Article 23 of the Convention,³²⁰ as well as the corruption of children according to Article 22. Furthermore, the Lanzarote Committee³²¹ also considers evolving trends such as self-generated images and material, sexual coercion and extortion, live streaming of child sexual abuse, sexting, bad hosting, anonymity and encryption of data/use of the dark net. As a result, the second

monitoring round of the Committee will be dedicated to the “Protection of children against ICT facilitated sexual exploitation and sexual abuse”.³²²

Similar to the Budapest Convention, the Lanzarote Convention also criminalises attempting and aiding and abetting the offences defined in the Convention (Article 24), while also addressing the issue of corporate responsibility (Article 26) and international cooperation (Article 38). Since cooperation helps countries identify and analyse problems, develop and apply common solutions, share data and expertise, combat impunity and improve prevention and protection measures, the Lanzarote Convention is open for signature by the member States, the non-member States which have participated in its elaboration and by the European Union, and is open for accession by other non-member States.³²³ To date it has been signed by all 47 member States of the Council of Europe and ratified by 42.³²⁴ Finally, the Lanzarote Committee organises capacity building activities and facilitates the exchange of good practice on the implementation of the Convention.

Gioia Scappucci, Executive Secretary of the Lanzarote Committee, Interview 23/02/2017

“*Harmonization is a way of clearly stating what the common ground is. In order to effectively fight against the crime, countries need to understand what they are combating. If crimes are defined in a harmonised way, the task is easier. [...] And that is why the Convention is open not only to the Council of Europe member States but also to any other country in the world. Child sexual abuse and exploitation is a transnational crime, a global concern. Offenders are everywhere, victims are everywhere, it's not question of territoriality. Therefore, the more countries are speaking the same language, agree what constitutes a crime, how that crime can be prosecuted or how the offenders can be looked for, the better to eradicate the crime. The more countries join the better.*”

EUROPEAN UNION DIRECTIVE ON COMBATING THE SEXUAL ABUSE AND SEXUAL EXPLOITATION OF CHILDREN AND CHILD PORNOGRAPHY, 2011

The Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA,³²⁵ harmonises throughout the European Union (EU) criminal offences relating to sexual abuse committed against children, the sexual exploitation of children, child pornography, grooming and sex tourism. It also lays down the minimum sanctions.³²⁶ Furthermore, it aims to prevent child sex offenders already convicted of an offence from exercising professional activities involving regular contact with children. Overall, compared to the Lanzarote Convention, the Directive establishes more explicit guidelines for criminal legislation regarding the sexual abuse and exploitation of children.³²⁷

With regard to forms of sexual abuse and sexual exploitation of children facilitated by the use of information and communication technology, such as the online solicitation of children for sexual purposes via social networking websites and chat rooms, the Directive stresses that they should be subject to effective, proportionate and dissuasive penalties.³²⁸ Furthermore, in order to reduce the circulation of child sexual abuse material on the Internet, the Directive requires Member States to remove websites containing such material hosted in their territory or in non-Member States, and, where appropriate, to block access to these sites in their territory.³²⁹

Of the 28 Member States of the European Union,³³⁰ 27 have transposed the Directive into their national law.³³¹

AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, 2014

The African Union Convention on Cyber Security and Personal Data Protection,³³² also known as the Malabo Convention, calls for the establishment of an appropriate normative framework on cyber-security and personal data protection, consistent with the African legal, cultural, economic and social environment. The goal of the Convention is to address the need for harmonised legislation in the area of cyber security in Member States of the African Union, and to establish in each State Party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use.³³³

With regard to child sexual abuse and exploitation, including by means of information and communication technology, the Convention specifically includes child pornography and exposure of children to pornography. Article 1 defines child pornography as “*any visual depiction, including any photograph, film, video, image, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: a) the production of such visual depiction involves a minor; b) such visual depiction is a digital image, computer image, or computer-generated image where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child’s knowledge; c) such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct.*” Offences related to child pornography include the following activities, as described in Article 29(3)(1): “*a) [p]roduce, register, offer, manufacture,*

make available, disseminate and transmit an image or a representation of child pornography through a computer system; b) [p]rocure for oneself or for another person, import or have imported, and export or have exported an image or representation of child pornography through a computer system; c) [p]ossess an image or representation of child pornography in a computer system or on a computer data storage medium.” The same article also criminalises the act of facilitating or providing access to images, documents, sound or representation of pornographic nature to a child. Exposure of children to pornography captures aspects of grooming and sexual extortion of children; however, the Malabo Convention does not explicitly criminalise these offences.

Furthermore, the participation “*in an association formed or in an agreement established with a view to preparing or committing*” child pornography is a criminal offence.³³⁴ The Malabo Convention also addresses the criminal liability of legal persons,³³⁵ demands effective, proportionate and dissuasive sanctions³³⁶ and deals with the issue of international cooperation.³³⁷

To date, the Malabo Convention has been signed by eight AU Member States,³³⁸ while it has been ratified only by Senegal.³³⁹

2. STATUS OF REPERES PROGRAMME COUNTRIES

NATIONAL LEGISLATION

According to the International Centre for Missing & Exploited Children (ICMEC), and its report “Child Pornography: Model Legislation & Global Review”, which reviews the legislation addressing the issue of child pornography in 196 countries:³⁴⁰

- Benin, Burkina Faso, Ethiopia and Lebanon are among the 35 countries worldwide that have no legislation specifically addressing child pornography.³⁴¹
- Kenya, Mali, Niger and Rwanda are among the 60 countries whose legislation addressing child pornography does not provide a definition of child pornography.
- Ivory Coast, Mali and Niger are among the 26 countries whose legislation addressing child pornography does not provide for child pornography online.
- Tanzania and Togo has specific legislation for child pornography and child pornography online that provides a definition of child pornography.
- Madagascar, Morocco and Uganda additionally criminalise as child pornography the knowing possession of child pornography, regardless of intent to distribute. As such, these countries rank among the top 82 countries worldwide with sufficient legislation to combat child pornography offences.

INTERNATIONAL AND REGIONAL LEGISLATION

Benin, Burkina Faso, Ivory Coast, Ethiopia, Kenya, Lebanon, Madagascar, Mali, Morocco, Niger, Rwanda, Tanzania, Togo and Uganda are member states of international and regional organisations, and yet not party to all of their treaties, which would enable their governments to create a comprehensive legislative strategy against online child sexual abuse and exploitation.

Table of signatures and ratifications/accessions³⁴²

	CRC	ACRWC	ILO C182	OPSC	Budapest Convention	Lanzarote Convention	Malabo Convention
Benin	S: 1990 R/A: 1990	S: 27/02/1992 R/A: 17/04/1997	R: 06/11/2001	S: 2001 R/A: 2005			S: 28/01/2015 R/: NA
Burkina Faso	S: 1990 R/A: 1990	S: 27/02/1992 R/A: 08/06/1992	R: 25/07/2001	S: 2001 R/A: 2006			
Ethiopia	S: NA R/A: 1991	S: NA R/A: 02/10/2002	R: 02/09/2003	S: NA R/A: 2014			
Ivory Coast	S: 1990 R/A: 1991	S: 27/02/2004 R/A: 01/03/2002	R: 07/02/2003	S: NA R/A: 2011			
Kenya	S: 1990 R/A: 1990	S: NA R/A: 25/07/2000	R: 07/05/2001	S: 2000 R/A: NA			
Lebanon	S: 1990 R/A: 1991		R: 11/09/2001	S: 2001 R/A: 2004			
Madagascar	S: 1990 R/A: 1991	S: 27/02/1992 R/A: 30/03/2005	R: 04/10/2001	S: 2000 R/A: 2004			
Mali	S: 1990 R/A: 1990	S: 28/02/1996 R/A: 03/06/1998	R: 14/07/2000	S: NA R/A: 2002			
Morocco	S: 1990 R/A: 1993	S: NA R/A: NA	R: 26/01/2001	S: 2000 R/A: 2001	Invited to accede	Request for accession accepted	
Niger	S: 1990 R/A: 1990	S: 13/07/1999 R/A: 11/12/1996	R: 23/10/2000	S: 2002 R/A: 2004			
Rwanda	S: 1990 R/A: 1991	S: 02/10/1991 R/A: 11/05/2001	R: 23/05/2000	S: NA R/A: 2002			
Tanzania	S: 1990 R/A: 1991	S: 23/10/1998 R/A: 16/03/2003	R: 12/09/2001	S: NA R/A: 2003			
Togo	S: 1990 R/A: 1990	S: 27/02/1992 R/A: 05/05/1998	R: 19/09/2000	S: 2001 R/A: 2004			
Uganda	S: 1990 R/A: 1990	S: 26/02/1992 R/A: 17/08/1994	R: 21/06/2001	S: NA R/A: 2001			

S: Signature
R: Ratification
A: Accession

ENDNOTES

- ¹ Renforcement de la Protection des Enfants victimes et à Risques d'Exploitation Sexuelle
- ² Benin, Burkina Faso, Ethiopia, Ivory Coast, Kenya, Lebanon, Madagascar, Mali, Morocco, Niger, Rwanda, Tanzania, Togo and Uganda
- ³ ECPAT International, "Understanding African children's use of Information and Communication Technologies (ICTs)", January 2013, p. 4, www.ecpat.org/news/understanding-african-childrens-use-information-and-communication-technologies: In African countries, families do not usually have a PC in their houses; children's access to Internet is mainly through smartphones and in cybercafés.
- ⁴ According to a survey by Get Safe Online, about 25% of interviewed parents know that their children have disclosed personal information while online gaming and about 34% said that their children have spoken to someone they do not know while online gaming, www.getsafeonline.org/safeguarding-children/gaming/
- ⁵ See also, Internet Society, "Children and the Internet", www.internetsociety.org/sites/default/files/bp-childrenandtheinternet-20129017-en.pdf
- ⁶ ECPAT International and ECPAT Luxembourg, "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse", January 2016, p. 82, <http://luxembourgguidelines.org/english-version/>
- ⁷ National Society for the Prevention of Cruelty to Children (NSPCC), "Online child sexual abuse images. Doing more to tackle demand and supply", November 2016, p. 4. www.nspcc.org.uk/globalassets/documents/research-reports/online-child-sexual-abuse-images.pdf
- ⁸ International Association of Internet Hotlines INHOPE, www.inhope.org
- ⁹ Joint INSAFE-INHOPE Annual Report 2014, p. 7, www.inhope.org/Libraries/Annual_reports/Joint_Insafe_INHOPE_Annual_Report_2014.sflb.ashx?download=true
- ¹⁰ INHOPE, "Statistics 2014", www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx
- ¹¹ The NetClean Report 2016, "Ten important insights into child sexual abuse crime". A report about child sexual abuse crime – based on a survey from 370 police officers in 26 countries, p. 15, www.netclean.com/wp-content/uploads/2016/12/NetClean_Report_2016_English_print.pdf; See also, Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2016", p. 26, www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
- ¹² Björn Sellström, Swedish Police, National Operative Department (NOA), Swedish Cyber Crime Centre, the Child Sexual Abuse Group, at The NetClean Report 2016, op. cit., p. 15
- ¹³ Internet World Stats, "World Internet Usage and Population Statistics", March 25, 2017, www.internetworldstats.com/stats.html
- ¹⁴ ECPAT International, "The commercial sexual exploitation of children in Africa. Developments, progress, challenges and recommended strategies", November 2014, p. 20, www.ecpat.org/wp-content/uploads/legacy/Regional%20CSEC%20Overview_Africa.pdf

- ¹⁵ ECPAT France et ECPAT Luxembourg, “Rapport Global de suivi de la mise en oeuvre des actions de lutte contre l’exploitation sexuelle des enfants à des fins commerciales: Burkina Faso”, troisième édition, p. 17, www.ecpat.org/wp-content/uploads/2016/04/A4A_V2_AF_BURKINA-FASO_2016.pdf
- ¹⁶ ECPAT International, “Global monitoring status of action against commercial sexual exploitation of children: Uganda”, 2nd Edition, p. 16, www.ecpat.org/wp-content/uploads/2016/04/a4a_v2_af_uganda_o.pdf
- ¹⁷ Terre des Hommes Netherlands, “Money Makes the World Go Down. Child Sexual Abuse and Child Sexual Exploitation in Tanzania”, May 2009, p. 11, www.menshandelweb.nl/system/files/documents/14%20feb%202014/Money%20Makes%20the%20World%20Go%20Down%20%20Tanzania.pdf
- ¹⁸ National Network of Organizations Working with Children (NNOC), “Non-Government Organisations’ Report on the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography in Tanzania”, May 2008, p. 31, www.crin.org/en/docs/Tanzania_NNOC_OPSC_NGO_Report.pdf
- ¹⁹ Uganda Youth Development Link (UYDEL), “Commercial Sexual Exploitation of Children in Uganda. A critical review of efforts to address CSEC 2005 – 2011”, May 2011, p. 67, <https://ssa.riselearningnetwork.org/wp-content/uploads/sites/5/2015/12/CSEC-in-Uganda-2011-UYDEL-booklet-23-08-2011pdf-20111206-115302.pdf>
- ²⁰ INTERPOL, “Appropriate Terminology”, www.interpol.int/Crime-areas/Crimes-against-children/Appropriate-terminology
- ²¹ See, for instance, Convention on the Rights of the Child (CRC), Article 1; African Charter on the Rights and Welfare of the Child (ACRWC), Article 2; International Labour Organization (ILO) Convention No. 182 on the Worst Forms of Child Labour (ILO C182), Article 2; Council of Europe Convention on Cybercrime (Budapest Convention), Article 9(3); Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), Article 3(a); ECPAT International and ECPAT Luxembourg, op. cit., p. 5-6
- ²² Lanzarote Convention, Article 18(1a); Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (Directive 2011/93/EU), Article 2(b)
- ²³ International Centre for Missing & Exploited Children (ICMEC), “Child Pornography: Model Legislation & Global Review”, 8th edition, 2016, p. 1, www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf
- ²⁴ ECPAT International and ECPAT Luxembourg, op. cit., p. 7-8
- ²⁵ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.201, Lanzarote, 25/10/2007, Entry into force 01/07/2010, www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084822
- ²⁶ Article 18(3) sets forth that Article 18(1a) does not cover consensual sexual activity between children.
- ²⁷ ECPAT International and ECPAT Luxembourg, op. cit., p. 19-20
- ²⁸ NSPCC, “Child Sexual Abuse. An NSPCC research briefing”, July 2013, p. 2. www.nspcc.org.uk/globalassets/documents/information-service/research-briefing-child-sexual-abuse.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCf%3d%3d&_t_q=non-contact+child+sexual+abuse&_t_tags=language%3aen%2csiteid%3a7f1b9313-bf5e-4415-abf6-aaf87298c667&_t_ip=46.193.65.111&_t_hit_id=Nspcc_Web_Models_Media_GenericMedia/_1d9843cb-af4b-412d-be2d-b76326379cf1&_t_hit_pos=3; See also, Lanzarote Committee, “1st implementation report, Protection of children

against sexual abuse in the circle of trust, The Framework”, T-ES(2015)05_en final, 8 January 2016, p. 17, <https://rm.coe.int/168058cdfd>: “The Lanzarote Committee: Invites Parties to review their legislation to address all serious harm to the sexual integrity of children by not limiting their criminal offences to sexual intercourse or equivalent acts (R9).”

- ²⁹ ECPAT International and ECPAT Luxembourg, op. cit., p. 24-25
- ³⁰ UNICEF, UNESCAP and ECPAT, “Commercial Sexual Exploitation of Children (CSEC) and Child Sexual Abuse (CSA) in the Pacific: A Regional Report”, 2006, p. 15, www.unicef.org/eapro/Pacific_CSEC_report.pdf: Children who have reached the age of 13 but have not yet reached age 18 may be referred to on occasion as “youth” or “young people”, while still being included in the broad definition of children.
- ³¹ African Charter on the Rights and Welfare of the Child (ACRWC), Adopted by the 26th Ordinary Session of the Assembly of Heads of State and Government of the OAU, Addis Ababa, Ethiopia - July 1990 (in 2001, the OAU legally became the African Union), entered into force Nov. 29, 1999, OAU Doc. CAB/LEG/24.9/49 (1990), www.acerwc.org/download/the-charter-english/?wpdmdl=8410
- ³² Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093> (Note that the Directive is wrongly referred to as 2011/92/EU on the Eur-lex website)
- ³³ ECPAT International and ECPAT Luxembourg, op. cit., p. 24
- ³⁴ Ibid, p. 25
- ³⁵ Ibid., p. 22
- ³⁶ Ibid.: “Unwanted sexual comments” can be a form of sexual harassment. The process of sexual abuse may include or even start with unwanted sexual comments on, for instance, the way the child is dressed or is using make-up or on her/his physical beauty, thus embarrassing the child. While such comments do not always lead to sexually abusive activities, they may still cause harm to the child, and may be considered a form of non-contact abuse, case in which the abuser does not have physical contact with the child.
- ³⁷ Ibid., p. 23: Case in which online child sexual abuse becomes exploitation; For more details, see also paragraph on “Online child sexual exploitation”
- ³⁸ NSPCC, “What is online abuse”, www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/
- ³⁹ ECPAT International and ECPAT Luxembourg, op. cit., p. 27
- ⁴⁰ NSPCC, “What is child sexual exploitation”, www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-sexual-exploitation/
- ⁴¹ ECPAT International and ECPAT Luxembourg, op. cit., p. 28
- ⁴² The European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC) brings together key actors from law enforcement, the private sector and civil society in Europe with the common goal of fighting the commercial sexual exploitation of children online. Members of the EFC join forces to take action on the payment and ICT systems that are used to run these illegal operations.
- ⁴³ European Cybercrime Centre (EC3) – Europol, “EFC Commercial Sexual Exploitation of Children Online, A Strategic Assessment”, 2015, p. 7, www.europol.europa.eu/publications-documents/commercial-sexual-exploitation-of-children-online

- ⁴⁴ European Cybercrime Centre (EC3) – Europol, “Virtual Global Taskforce Child Sexual Exploitation Environmental Scan 2015”, p. 21, www.europol.europa.eu/newsroom/news/2015-vgt-child-sexual-exploitation-environmental-scan
- ⁴⁵ ECPAT International and ECPAT Luxembourg, op. cit., p. 35-36
- ⁴⁶ Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002, www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx
- ⁴⁷ The expression «*for primarily sexual purposes*» excludes and thus does not consider as “child pornography” for example, material having a medical, scientific merit, i.e. where there is absence of sexual purposes, whereas the same material (re)produced for a pornographic website may be deemed child pornography.
- ⁴⁸ More references to/definitions and constitutive elements of child pornography in legally binding instruments: CRC, Article 34(c); ACRWC, Article 27(c); ILO C182, Article 3(b); Budapest Convention, Article 9(1-2); Directive 2011/93/EU, Articles 2(c) and 5; African Union Convention on cyber security and personal data protection (Malabo Convention), Articles 1 and 29(3.1(a-c))
- ⁴⁹ INTERPOL is the world’s largest international police organization, with 190 member countries, www.interpol.int
- ⁵⁰ INTERPOL, “Appropriate Terminology”, op. cit.
- ⁵¹ European Police Office (Europol) is the European Union’s law enforcement agency, www.europol.europa.eu
- ⁵² ECPAT International and ECPAT Luxembourg, op. cit., p. 39
- ⁵³ See also, International Telecommunication Union (ITU) and United Nations Children’s Fund (UNICEF), “Guidelines for Industry on Child Online Protection”, 2015 edition, p. 29, www.unicef.org/csr/files/COP_Guidelines_English.pdf; European Parliament resolution of 11 March 2015 on child sexual abuse online (2015/2564(RSP)), Paragraph 12, www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2015-0070&language=EN
- ⁵⁴ ECPAT International and ECPAT Luxembourg, op. cit., p. 40
- ⁵⁵ Ibid., p. 36
- ⁵⁶ Material that represents persons 18 years of age or older in child-like poses, to appear as if children are depicted; Budapest Convention, Article 9(2)(b) and Directive 2011/93/EU, Article 2(c)(iii)
- ⁵⁷ For more details, see also paragraph on “Computer/digitally generated child sexual abuse material”
- ⁵⁸ For more details, see also paragraph on “Self-generated sexual material”
- ⁵⁹ For more details, see also paragraph on “Sexualised images of children”
- ⁶⁰ ECPAT International and ECPAT Luxembourg, op. cit., p. 41: A “pseudo photograph” is “an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph”. Such photographs, which are also sometimes referred to as “morphed” or “blended” images, are created by digitally combining a number of photographs or portions of photographs (often of children and adults) to create an individual image. In the days before computer-aided photo editing was available, offenders would place the picture of the head of a child about whom they were fantasising onto that of the naked body of an adult or another child.
- ⁶¹ Ibid.

- ⁶² ECPAT International, “Protection and the OPSC: Justifying Good Practice Laws to Protect Children from Sexual Exploitation”, Journal Series No. 2, April 2012, p. 18-20, www.ecpat.org/wp-content/uploads/legacy/ecpat_journal_apr2012_final.pdf
- ⁶³ Convention on Cybercrime, ETS No.185, Budapest, 23/11/2001, Entry into force 01/07/2004, www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
- ⁶⁴ ECPAT International and ECPAT Luxembourg, op. cit., p. 40
- ⁶⁵ Ibid., footnote 177
- ⁶⁶ Ibid., p. 41
- ⁶⁷ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 13
- ⁶⁸ Europol, “IOCTA 2016”, op. cit., p. 25
- ⁶⁹ The NetClean Report 2016, op. cit., p. 19
- ⁷⁰ Ibid., p. 18
- ⁷¹ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 6
- ⁷² Internet Watch Foundation (IWF) and Microsoft, “Emerging Patterns and Trends Report#1, Online-Produced Sexual Content”, March 2015, p. 17, www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf : For the purposes of the study, 3,803 images and videos were assessed over a three month period between September and November 2014.
- ⁷³ The NetClean Report 2016, op. cit., p. 19
- ⁷⁴ As part of sexting
- ⁷⁵ ECPAT International and ECPAT Luxembourg, op. cit., p. 43
- ⁷⁶ Ibid.
- ⁷⁷ Ibid.
- ⁷⁸ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 14; For more examples, see also, ECPAT International and ECPAT Luxembourg, op. cit., p. 43, footnote 189
- ⁷⁹ ECPAT International and ECPAT Luxembourg, op. cit., p. 44
- ⁸⁰ NSPCC, “What is sexting?”, www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/?t_id=1B2M2Y8AsgTpgAmY7PhCfg%3d%3d&t_q=sexting&t_tags=language%3aen%2csiteid%3a7f1b9313-bf5e-4415-abf6-aaf87298c667&t_ip=46.193.167.114&t_hit.id=Nspcc_Web_Models_Pages_StandardPage/_a5245587-27cb-42c6-8830-0657efe408f6_en-GB&t_hit.pos=1
- ⁸¹ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 9
- ⁸² ECPAT International and ECPAT Luxembourg, op. cit., p. 44
- ⁸³ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 9-10
- ⁸⁴ ECPAT International and ECPAT Luxembourg, op. cit., p. 44
- ⁸⁵ Missing Children Europe, ECPAT and eNASCO, “Together against sexual exploitation of children:

Survey on the transposition of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography”, 2015, p. 20, <http://missingchildreurope.eu/Portals/0/Docs/A%20survey%20on%20transposition%20of%20Directive%20against%20child%20sexual%20exploitation%20and%20abuse.pdf>

- ⁸⁶ Serious Crime Act 2015, Section 67, www.legislation.gov.uk/ukpga/2015/9/section/67/enacted
- ⁸⁷ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 12
- ⁸⁸ See, for instance, “Operation Koala” at Eurojust, “Worldwide child sex offender network dismantled”, Press Release 5 November 2007, www.eurojust.europa.eu/press/pressreleases/pages/2007/2007-11-05.aspx
- ⁸⁹ ECPAT International and ECPAT Luxembourg, op. cit., p. 42
- ⁹⁰ ECPAT International and ECPAT Luxembourg, op. cit., p. 46: The recruitment and use of a child for participation in any type of pornographic performances, whether online or offline, must be criminalised in accordance with the CRC (Article 34(c)), the ACRWC (Article 27(c)), ILO C182 (Article 3(b)), and the Lanzarote Convention (Article 21). Moreover, it could fall under the OPSC definition of “child prostitution”: “*the use of a child in sexual activities for remuneration or any other form of consideration*” (Article 2(b)). When the live performance by the child is recorded or registered, this can amount to the production of child sexual abuse material, also covered by all major legal instruments under child pornography provisions.
- ⁹¹ Ibid., p. 46-47
- ⁹² Europol, “IOCTA 2016”, op. cit., p. 26
- ⁹³ ECPAT International and ECPAT Luxembourg, op. cit., p. 47
- ⁹⁴ Europol, “IOCTA 2016”, op. cit., p. 26
- ⁹⁵ The NetClean Report 2016, op. cit., p. 26
- ⁹⁶ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 6
- ⁹⁷ Europol, “IOCTA 2016”, op. cit., p. 26, The NetClean Report 2016, op. cit., p. 15
- ⁹⁸ ECPAT International and ECPAT Luxembourg, op. cit., p. 47-48
- ⁹⁹ Ibid., p. 49
- ¹⁰⁰ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 3
- ¹⁰¹ Ibid., p. 4
- ¹⁰² ECPAT International and ECPAT Luxembourg, op. cit., p. 50
- ¹⁰³ Currently, the Lanzarote Convention is the only legally binding international (beyond EU countries) instrument that contains an obligation to criminalise the solicitation of children for sexual purposes. For such criminalisation, “*the intentional proposal, through information and communication technologies, of an adult to meet a child*” is required (Article 23). However, the Lanzarote Committee adopted an opinion in June 2015 on Article 23, which states that “*[t]he overall phenomenon of online grooming evolves in parallel to information and communication technologies. Its understanding should therefore not restrict itself to the way online grooming was committed when the Convention was drafted, but should be understood and tackled according to how it is being committed today and could be committed tomorrow. As no static definition of online grooming is possible, Parties should consider extending its criminalisation also to cases when the sexual abuse is not the result of a meeting in person, but is committed*

online.” (Lanzarote Committee, Committee of the Parties to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (T-ES), “Opinion on Article 23 of the Lanzarote Convention and Its Explanatory Note”, 23 June 2015, Paragraph 20, <https://rm.coe.int/168046ebc8>)

- ¹⁰⁴ Explanatory Memorandum, Criminal Law (Child Grooming) Bill 2014, Ireland, p. 2, www.oireachtas.ie/documents/bills28/bills/2014/8914/b8914d-memo.pdf
- ¹⁰⁵ ECPAT International and ECPAT Luxembourg, op. cit., p. 52-53; EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 25-26
- ¹⁰⁶ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 24
- ¹⁰⁷ ECPAT International and ECPAT Luxembourg, op. cit., p. 44
- ¹⁰⁸ Ibid., p. 45, footnote 200
- ¹⁰⁹ Children’s Commissioner for England, “We call for urgent action to protect children from exposure to pornography”, Press Release 24 May 2013, www.childrenscommissioner.gov.uk/news/we-call-urgent-action-protect-children-exposure-pornography
- ¹¹⁰ ECPAT Luxembourg, “NGO Report on 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 in Luxembourg”, p. 14-15, http://tbinternet.ohchr.org/Treaties/CRC-OP-SC/Shared%20Documents/LUX/INT_CRC-OP-SC_NGO_LUX_21359_E.pdf
- ¹¹¹ For instance, Lanzarote Convention, Article 22: “Each Party shall take the necessary legislative or other measures to criminalise the intentional causing, for sexual purposes, of a child who has not reached the age set in application of Article 18, paragraph 2, to witness sexual abuse or sexual activities, even without having to participate.”; ECPAT International and ECPAT Luxembourg, op. cit., p. 45
- ¹¹² See, for instance, www.oregonlaws.org/ors/163.432
- ¹¹³ ECPAT International and ECPAT Luxembourg, op. cit., p. 45
- ¹¹⁴ International Centre for Missing & Exploited Children (ICMEC), “Framing Implementation: A Supplement to Child Pornography: Model Legislation & Global Review”, 2017, p. 3, www.icmec.org/wp-content/uploads/2017/02/Framing-Implementation_2017.pdf
- ¹¹⁵ WePROTECT Global Alliance, “Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response”, November 2016, p. 3, <https://static1.squarespace.com/static/5630f48de4b00a75476ecfoa/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>
- ¹¹⁶ The WePROTECT Global Alliance to End Child Sexual Exploitation Online combines two major initiatives: the Global Alliance, led by the U.S. Department of Justice and the EU Commission and WePROTECT, which was convened by the UK, www.weprotect.org
- ¹¹⁷ WePROTECT Global Alliance, op. cit., p. 1
- ¹¹⁸ Ibid., p. 2
- ¹¹⁹ Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with article 49, www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx
- ¹²⁰ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 2-3

- ¹²¹ Missing Children Europe, ECPAT and eNASCO, op. cit., p. 22
- ¹²² ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 3; Greek Criminal Code, Article 348A(1)
- ¹²³ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 9; Directive 2011/93/EU, Article 14
- ¹²⁴ ECPAT International and ECPAT Luxembourg, op. cit., p. 89
- ¹²⁵ Lanzarote Convention, Article 33: “Each Party shall take the necessary legislative or other measures to ensure that the statute of limitation for initiating proceedings with regard to the offences established in accordance with Articles 18, 19, paragraph 1.a and b, and 21, paragraph 1.a and b, shall continue for a period of time sufficient to allow the efficient starting of proceedings after the victim has reached the age of majority and which is commensurate with the gravity of the crime in question.”; Explanatory Report to the Lanzarote Convention, Paragraph 231, <https://rm.coe.int/16800d3832>: “Indeed, it is acknowledged that many child victims of sexual abuse are unable, for various reasons, to report the offences perpetrated against them before reaching the age of majority.”; Directive 2011/93/EU, Article 15(2)
- ¹²⁶ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 6-8; See also, data preservation measures under the Budapest Convention, Articles 16 and 17.
- ¹²⁷ For more details, see also paragraph on “Investigatory tools”
- ¹²⁸ Directive 2011/93/EU, Article 25
- ¹²⁹ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., 2016, p. 5; For more details, see also paragraph on “Reporting online child sexual abuse and exploitation”
- ¹³⁰ Under the dual criminality requirement, when a crime committed abroad must also be a crime in an offender’s home country in order for the offender to be prosecuted in her/his home country.
- ¹³¹ Sweden, Ministry of Health and Social Affairs, “National Action Plan for Safeguarding Children from Sexual Exploitation”, Article no. S.2008.024, September 2008, op. cit., p. 11, www.government.se/49b757/contentassets/fb78975ee42f41349f782189fbee929a/national-action-plan-for-safeguarding-children-from-sexual-exploitation
- ¹³² The OPSC demands, in Article 9(2), that States Parties “promote in the public at large, including children, through information by all appropriate means, education and training, about the preventive measures and harmful effects” of child sexual exploitation and child pornography. The Lanzarote Convention requires, in Article 8(1), that Member States “promote or conduct awareness raising campaigns addressed to the general public providing information on the phenomenon of sexual exploitation and sexual abuse of children and on the preventive measures which can be taken.” The Directive 2011/93/EU (Article 23(2) and Recital 34) calls for the establishment of policies to prevent sexual abuse and sexual exploitation of children by means of information and awareness raising campaigns, research and education programmes. Awareness raising campaigns addressed to children should be “appropriate and sufficiently easy to understand.”
- ¹³³ International Telecommunication Union (ITU), “Guidelines for Parents, Guardians and Educators on Child Online Protection”, Second Edition 2016, p. 7, www.itu.int/en/cop/Documents/S-GEN-COP.EDUC-2016-PDF-E%5B1%5D.pdf
- ¹³⁴ Sweden, Ministry of Health and Social Affairs, op. cit., p. 20
- ¹³⁵ ITU, “Guidelines for Parents, Guardians and Educators on Child Online Protection”, op. cit., p. 6
- ¹³⁶ ECPAT International, “Understanding African children’s use of Information and Communication Technologies (ICTs)”, op. cit., p. 32

- ¹³⁷ ITU and UNICEF, op. cit., p. 29
- ¹³⁸ ECPAT International, “Understanding African children’s use of Information and Communication Technologies (ICTs)”, op. cit., p. 31
- ¹³⁹ ITU, “Guidelines for Parents, Guardians and Educators on Child Online Protection”, op. cit., p. 35; See also, Family Online Safety Institute (FOSI), “Parents, Privacy and Technology Use”, November 2015, www.fosi.org/policy-research/parents-privacy-technology-use/
- ¹⁴⁰ ITU, “Guidelines for Parents, Guardians and Educators on Child Online Protection”, op. cit., p. 7
- ¹⁴¹ ECPAT International, “Understanding African children’s use of Information and Communication Technologies (ICTs)”, op. cit., p. 32
- ¹⁴² International Telecommunications Union (ITU), “Guidelines for Policy Makers on Child Online Protection”, 2009, p. 38, www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf
- ¹⁴³ Office of the UN Special Representative of the Secretary-General on Violence against Children, “Releasing children’s potential and minimizing risks ICTs, the Internet and Violence against Children”, New York, 2014, p. 48, http://srg.violenceagainstchildren.org/sites/default/files/publications_final/icts/releasing_children_potential_and_minimizing_risks_icts_the_internet_and_violence_against_children.pdf
- ¹⁴⁴ WePROTECT Global Alliance, op. cit., p. 24
- ¹⁴⁵ Ibid., p. 24; Sweden, Ministry of Health and Social Affairs, op. cit., p. 19
- ¹⁴⁶ Europol, “IOCTA 2016”, op. cit., p. 13
- ¹⁴⁷ ITU, “Guidelines for Policy Makers on Child Online Protection”, p. 43
- ¹⁴⁸ ICMEC, “Framing Implementation: A Supplement to Child Pornography: Model Legislation & Global Review”, op. cit., p. 10
- ¹⁴⁹ November 20th is the date in 1959 when the UN General Assembly adopted the Declaration of the Rights of the Child. It is also the date in 1989 when the UN General assembly adopted the Convention on the Rights of the Child, www.un.org/en/events/childrenday
- ¹⁵⁰ This occasion is firstly a commemoration to recall the 1976 uprising in Soweto, when a protest by school children in South Africa against apartheid –inspired education resulted in the public killing of these unarmed young protesters by police officials. The Day of the African Child is celebrated since 1991 and every year a theme is identified by the African Committee of Experts on the Rights and Welfare of the Child. In 2016, the Day was on the theme “Conflict and Crisis in Africa: Protecting all Children’s Rights”, www.africawidemovement.org/en/index.php/30-announcements/other-information/178-day-of-the-african-child-2016
- ¹⁵¹ Starting as an initiative of the EU SafeBorders project in 2004 and taken up by the Insafe network, the Safer Internet Day promotes a safer and more responsible use of online technology and mobile phones by children and young people across the world (www.saferinternetday.org). It is celebrated in more than 100 countries worldwide. Among them, formal SID Committees operate in Kenya, Lebanon and Uganda.
- ¹⁵² Established by the Council of Europe in 2015, www.coe.int/en/web/children/end-child-sex-abuse-day; The 2017 edition of the European Day will focus on online child sexual exploitation and sexual abuse.
- ¹⁵³ ECPAT France, http://ecpat-france.fr/centre_ressources/1-outils_ecpat/1-ECPAT_France/1-campagnes_information/1-campagne_2009/3-Lutte_contre_la_pedopornographie/affiche/ECPA_0903033_Chambr_210x297_N300_CMYK.pdf

- ¹⁵⁴ <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/>
- ¹⁵⁵ Say No! - A campaign against online sexual coercion and extortion of children by Europol, www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime
- ¹⁵⁶ See, for example, OPSC, Article 8(4); Lanzarote Convention, Articles 5(2) and 36(1); Directive 2011/93/EU Article 23(3)
- ¹⁵⁷ Sweden, Ministry of Health and Social Affairs, op. cit., p. 10 and 15
- ¹⁵⁸ ICMEC, “Framing Implementation: A Supplement to Child Pornography: Model Legislation & Global Review”, op. cit., p. 10
- ¹⁵⁹ www.interpol.int/INTERPOL-expertise/Training-and-capacity-building
- ¹⁶⁰ The 17th Europol training course on “Combating the Online Sexual Exploitation of Children on the Internet” (COSEC), held in Selm, Germany, in October 2016, provided training for 65 representatives from EU Member States, non-EU States (Albania, Australia, Canada, Colombia, Israel, the Former Yugoslav Republic of Macedonia, Moldova, New Zealand, Norway, Serbia, Switzerland, Ukraine and the United States), Europol and Interpol, www.europol.europa.eu/newsroom/news/17th-europol-training-course-%E2%80%98combating-online-sexual-exploitation-of-children-internet%E2%80%99
- ¹⁶¹ Cybercrime Programme Office of the Council of Europe (C-PROC), www.coe.int/en/web/cybercrime/cybercrime-office-c-proc; For more details, see also, ANNEX paragraph on “Council of Europe Convention on Cybercrime, 2001”
- ¹⁶² European Judicial Training Network (EJTN), www.ejtn.eu
- ¹⁶³ International Federation of Social Workers (IFSW), <http://ifsw.org/>
- ¹⁶⁴ IFSW, “Guiding Principles for Social Workers Working with Others to Identify and Protect Children From all Forms of Sexual Abuse,” Policy statement, October 2014, http://cdn.ifsw.org/assets/ifsw_103737-2.pdf
- ¹⁶⁵ <http://ifsw.org/membership/our-members/>
- ¹⁶⁶ Global Social Service Workforce Alliance, www.socialserviceworkforce.org
- ¹⁶⁷ www.socialserviceworkforce.org/map
- ¹⁶⁸ Stop It Now!, www.stopitnow.org
- ¹⁶⁹ Lucy Faithfull Foundation, www.lucyfaithfull.org.uk
- ¹⁷⁰ Kein Täter Werden (Don’t offend), www.dont-offend.org
- ¹⁷¹ Directive 2011/93/EU Article 10(1) and Recital 40
- ¹⁷² Lanzarote Convention, Article 5(3): “Each Party shall take the necessary legislative or other measures, in conformity with its internal law, to ensure that the conditions to accede to those professions whose exercise implies regular contacts with children ensure that the candidates to these professions have not been convicted of acts of sexual exploitation or sexual abuse of children.”
- ¹⁷³ Directive 2011/93/EU, Article 10(2): “Member States shall take the necessary measures to ensure that employers, when recruiting a person for professional or organised voluntary activities involving direct and regular contacts with children, are entitled to request information in accordance with national law by way of any appropriate means, such as access upon request or

via the person concerned, of the existence of criminal convictions for any of the offences referred to in Articles 3 to 7 entered in the criminal record or of the existence of any disqualification from exercising activities involving direct and regular contacts with children arising from those criminal convictions.”

- ¹⁷⁴ Missing Children Europe, ECPAT and eNASCO, op. cit., p. 33-35, 40
- ¹⁷⁵ Ibid., p. 28-32; Directive 2011/93/EU, Recital 43; European Parliamentary Research Service (EPRS), “Combating sexual abuse of children Directive 2011/93/EU, European Implementation Assessment”, PE 598.614, April 2017, p. 41-44, [www.europarl.europa.eu/RegData/etudes/STUD/2017/598614/EPRS_STU\(2017\)598614_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598614/EPRS_STU(2017)598614_EN.pdf)
- ¹⁷⁶ ICMEC, “Framing implementation: A supplement to Child Pornography: Model Legislation & Global Review”, op. cit., p. 11
- ¹⁷⁷ UN Special Rapporteur on the sale and sexual exploitation of children, www.ohchr.org/EN/Issues/Children/Pages/ChildrenIndex.aspx; For more details, see also, ANNEX, paragraph on “United Nations Convention on the Rights of the Child, 1989”
- ¹⁷⁸ UNICEF, www.unicef.org
- ¹⁷⁹ UNICEF Office of Research – Innocenti, www.unicef-irc.org
- ¹⁸⁰ Lanzarote Committee, www.coe.int/en/web/children/lanzarote-committee; For more details, see also, ANNEX, paragraph on “Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 2007”
- ¹⁸¹ ICMEC, “Framing implementation: A supplement to Child Pornography: Model Legislation & Global Review”, op. cit., p. 12
- ¹⁸² ECPAT International, www.ecpat.org; There are 95 ECPAT members in 86 countries across all regions of the world, www.ecpat.org/where-we-work
- ¹⁸³ www.icmec.org/child-pornography-model-legislation
- ¹⁸⁴ GRID, www.fosigrid.org
- ¹⁸⁵ Crimes Against Children Research Center, University of New Hampshire, www.unh.edu/ccrc/index.html
- ¹⁸⁶ International Centre, University of Bedfordshire, www.beds.ac.uk/ic
- ¹⁸⁷ WePROTECT Global Alliance, op. cit., p. 9
- ¹⁸⁸ Lanzarote Convention, Article 34(1): *“Each Party shall adopt such measures as may be necessary to ensure that persons, units or services in charge of investigations are specialised in the field of combating sexual exploitation and sexual abuse of children or that persons are trained for this purpose. Such units or services shall have adequate financial resources.”*
- ¹⁸⁹ Lanzarote Convention, Article 30(1 and 2); For more details, see also paragraph on “Child-friendly justice”
- ¹⁹⁰ WePROTECT Global Alliance, op. cit., p. 9
- ¹⁹¹ For example, Thorn, www.wearethorn.org; For more details, see also paragraph on “Developing innovative solutions”
- ¹⁹² For example, Financial Coalition Against Child Pornography (FCACP), www.missingkids.com/FCACP and www.icmec.org/fcACP; For more details, see also paragraph on “Industry engagement”

- ¹⁹³ INHOPE, www.inhope.org; For more details, see also paragraph on “Reporting online child sexual abuse and exploitation”
- ¹⁹⁴ Dr. Victoria Baines, “Online Child Sexual Abuse: The Law Enforcement Response”, A contribution of ECPAT International to the World Congress III against the Sexual Exploitation of Children and Adolescents, Rio de Janeiro, Brazil, 25–28 November 2008, p. 22, www.childcentre.info/public/Thematic_Paper_ICTLAW_ENG.pdf
- ¹⁹⁵ CEOP command, <https://ceop.police.uk/safety-centre/>; www.nationalcrimeagency.gov.uk/about-us/what-we-do/child-exploitation-online-protection-ceop/
- ¹⁹⁶ WePROTECT Global Alliance, op. cit., p. 9
- ¹⁹⁷ INTERPOL, www.interpol.int
- ¹⁹⁸ www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children; For more details, see also paragraph on “Victim identification”
- ¹⁹⁹ Virtual Global Taskforce (VGT), <http://virtualglobaltaskforce.com/>
- ²⁰⁰ VGT member countries/agencies include: Australia, Canada, Colombia, Europol, INTERPOL, Netherlands, New Zealand, Philippines, Republic of Korea, United Arab Emirates, United Kingdom, United States of America, Switzerland
- ²⁰¹ VGT private sector partners include: Blackberry, Child Rescue Coalition (CRC), ECPAT, ICDDL ARABIA, ICMEC, INHOPE, International Justice Mission (IJM), KIK, Magnet Forensics, Microsoft Digital Crimes Unit, National Children’s Advocacy Center (NCAC), NCMEC, NetClean, PayPal, Telstra, The Code, Web-IQ, World Vision (WV), Ziuz
- ²⁰² Europol – European Cybercrime Centre (EC3), www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
- ²⁰³ www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation
- ²⁰⁴ Algiers Declaration on the establishment of the African Mechanism for the Police Cooperation–AFRIPOL, February 2014, www.peaceau.org/uploads/algiers-declaration-afripol-english.pdf
- ²⁰⁵ www.peaceau.org/uploads/statement-consultative-meeting-afripol-2016.pdf
- ²⁰⁶ EC3 – Europol, “VGT Child Sexual Exploitation Environmental Scan 2015”, op. cit., p. 26; INTERPOL, “INTERPOL-coordinated operation strikes back at ‘sextortion’ networks”, News 02 May 2014, www.interpol.int/News-and-media/News/2014/N2014-075
- ²⁰⁷ The Lanzarote Convention, in Article 30(5) sets forth that “[s]pecialized units or investigative services should be enabled to identify victims of the offenses by analyzing child pornography material, specifically evidence such as photographs and audiovisual recordings transmitted or made available through the use of information and communication technologies.”; Directive 2011/93/EU, Article 15(4)
- ²⁰⁸ INTERPOL, “Victim identification”, www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification
- ²⁰⁹ INTERPOL, “INTERPOL network identifies 10,000 child sexual abuse victims”, News 09 January 2017, www.interpol.int/News-and-media/News/2017/N2017-001
- ²¹⁰ As of January 2017, 49 countries are connected to the ICSE database: Andorra, Argentina, Australia, Austria, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Moldova, Netherlands,

New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, United States and Vietnam. Europol is also connected to the database; The NetClean Report 2016, op. cit., p. 14

- ²¹¹ Project VIC, www.projectvic.org; The NetClean Report 2016, op. cit., p. 11 and 33
- ²¹² Microsoft PhotoDNA and F1 Video Fingerprinting; ECPAT International, “What are Hashes? What is PhotoDNA? And their application to child sexual abuse material”, ECPAT Internet & Technology Factsheet, www.ecpat.org/wp-content/uploads/legacy/IT%20Factsheet%20-%20What%20is%20PhotoDNA_o.pdf
- ²¹³ INTERPOL, “Global operation targets child sexual abuse material exchanged via messaging apps”, News 18 April 2017, www.interpol.int/News-and-media/News/2017/N2017-047
- ²¹⁴ WePROTECT Global Alliance, op. cit., p. 9
- ²¹⁵ PHAROS, Plateforme d’Harmonisation, d’Analyse, de Recoupement et d’Orientation des Signalements, www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil.input.action
- ²¹⁶ Yann VIELARD, International best practices, Benchmarking and Analysis, EU/COE Joint Project on Global Action on Cybercrime, 29-31 March 2017, Ghana, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680703a9f>
- ²¹⁷ Directive 2011/93/EU, Recital 27 and Article 15(3) combined with Article 5(1)
- ²¹⁸ ICMEC, “Framing implementation: A supplement to Child Pornography: Model Legislation & Global Review”, op. cit., p. 5, footnote 13
- ²¹⁹ Missing Children Europe, ECPAT and eNASCO, op. cit., p. 10, 13 and 44; Commitments and progress reports submitted by member countries of the Global Alliance Against Child Sexual Abuse Online at https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse_en
- ²²⁰ www.ohchr.org/EN/Issues/Children/Pages/SideEventHRC25.aspx
- ²²¹ French Criminal procedural code, Article 706-47-3
- ²²² Greek Criminal procedural code, Article 253A
- ²²³ UNICEF and GSMA, “Notice and Takedown: Company policies and practices to remove online child sexual abuse material”, May 2016, p. 5, www.unicef.org/csr/files/Notice_and_Takedown_English.pdf; Lanzarote Convention, Article 12(2) and Explanatory Report, Paragraph 91; Directive 2011/93/EU, Article 16(2) and Recital 28
- ²²⁴ ITU and UNICEF, op. cit., p. 17: ISPs act as both a conduit, providing access to and from the Internet, and a repository for data through their hosting, caching and storage services.
- ²²⁵ Verónica Donoso, INHOPE Executive Director, at The NetClean Report 2016, op. cit., p. 10: *“Hotlines are national focal points that allow the community to securely and anonymously report what they believe to be illicit material. Something they might otherwise feel uncomfortable or afraid to do directly to the police. Obviously, not all the content that is reported from the public is confirmed child sexual abuse material or illegal material. But this is exactly the added value of hotlines. By receiving and thoroughly analysing all these reports, including the non-illegal ones, hotlines save the police valuable time for victim and perpetrator identification and dismantling criminal networks. As a result, hotlines fill a gap that allows police to get access to information they would otherwise probably never have been able to find on their own.”*
- ²²⁶ ICMEC, “Framing implementation: A supplement to Child Pornography: Model Legislation & Global Review”, op. cit., p. 9

- ²²⁷ ITU and UNICEF, op. cit., p. 7, footnote 9
- ²²⁸ WePROTECT Global Alliance, op. cit., p. 23
- ²²⁹ INHOPE, www.inhope.org
- ²³⁰ INHOPE, Code of Practice, Version 4.0, May 2016, http://www.inhope.org/Libraries/Best_Practice_Papers/2016_Code_of_Practice_-_readopted_May_2016_AGM.sflb.ashx
- ²³¹ Internet Watch Foundation (IWF), www.iwf.org.uk
- ²³² Point de Contact, www.pointdecontact.net/?language=en
- ²³³ CyberTipline, www.missingkids.com/cybertipline
- ²³⁴ Australian Government, Office of the Children’s eSafety Commissioner, www.esafety.gov.au
- ²³⁵ Safer Internet Association (SIA) Japan, www.saferinternet.or.jp/english
- ²³⁶ www.inhope.org/gns/our-members
- ²³⁷ www.inhope.org/gns/our-members/SouthAfrica.aspx
- ²³⁸ IWF, “Our International Reporting Portal”, www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/our-international-reporting-portal; www.fosigrid.org/uganda
- ²³⁹ Europol, “International police action leads to rescue of 22-month old Romanian sex abuse victim”, Press Release 25 February 2015, www.europol.europa.eu/newsroom/news/international-police-action-leads-to-rescue-of-22-month-old-romanian-sex-abuse-victim
- ²⁴⁰ UNICEF and GSMA, op. cit., p. 7: A notice received from law enforcement or a hotline that asks a company to “take down” CSAM may be incorrectly perceived – it is important to understand that a takedown notice does not automatically mean a request to delete the material. “Takedown” means acting promptly to identify whether the reported material is illegal, and if so, to remove and isolate the content from being viewed or circulated by the public. Deleting CSAM may compromise an ongoing criminal investigation that is unknown to the company, and also prevent the identification of children who are being abused. If CSAM is confirmed, it should be securely isolated within the company’s networks and services and accessible only to those employees authorized to investigate and take action on CSAM reports. Companies should check the law applicable in their jurisdictions on handling child sexual abuse material.
- ²⁴¹ ITU and UNICEF, op. cit., p. 29
- ²⁴² WePROTECT Global Alliance, op. cit., p. 29; Directive 2011/93/EU, Article 25 and Recitals 46 and 47
- ²⁴³ ITU and UNICEF, op. cit., p. 7
- ²⁴⁴ EC3 – Europol, “EFC Commercial Sexual Exploitation of Children Online, A Strategic Assessment”, op. cit., p. 9: Once the report is received and assessed by the hotline as CSAM under its jurisdiction, it will normally be forwarded to the LEA (Process A) and/or the Internet Service Provider (ISP) (Process B). Content removal performed by a Content Service Provider (Process C) will follow where appropriate. Processes may differ between hotlines across the world based on their legal status, national law, as well as an agreement with LEA. In some cases, both LEA and ISP will be informed at the same time, whereas in other cases there will be a delay between the LEA and ISP.
- ²⁴⁵ Directive 2011/93/EU, Recital 47

- ²⁴⁶ INTERPOL, “Access blocking”, www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list; The decision to participate in this scheme must result from a policy decision within the ASP or be a result of legislation in the country of the ASP.
- ²⁴⁷ Lanzarote Convention, Article 12(2) and Explanatory Report, Paragraph 91; Directive 2011/93/EU, Article 16(2) and Recital 28
- ²⁴⁸ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 5
- ²⁴⁹ Lanzarote Convention, Article 12(1); Directive 2011/93/EU, Article 16(1)
- ²⁵⁰ WePROTECT Global Alliance, op. cit., p. 31; For instance, in France reporting for ISPs is mandatory under Law n° 2004-575, 21 June 2004, Article 6-I-7, al. 5
- ²⁵¹ WePROTECT Global Alliance, op. cit., p. 16
- ²⁵² ICMEC, “Framing Implementation: A Supplement to Child Pornography: Model Legislation & Global Review”, op. cit., p.
- ²⁵³ WePROTECT Global Alliance, op. cit., p. 21
- ²⁵⁴ Helplines within the Insafe network of Safer Internet Centres (SICs), www.betterinternetforkids.eu/web/portal/practice/helplines
- ²⁵⁵ Child Helpline International, www.childhelplineinternational.org
- ²⁵⁶ Directive 2011/93/EU, Article 19(3); Missing Children Europe, ECPAT and eNASCO, op. cit., p. 58-59
- ²⁵⁷ For instance, in Malta, every time an offence is reported, a meeting with different professionals is held to draw an individual welfare plan for the child victim. In Ireland, the Health Service Executive is required to assess the needs of the child to identify and offer appropriate support services based on a welfare plan. In Sweden, social services from each municipality shall establish an individual plan that meets the needs of the child victim. In Luxembourg, the “Enquête Sociale” aims at assessing the personality, mental condition and social environment of the child victim and to determine which measures are in their best interest. In the United Kingdom, the police and victims support services are required to undertake individual needs assessment for each victim and to adapt special measures to the needs identified. In Bulgaria, an assessment and a specific plan is made by a social worker. Their role through observation and consultation with the victim is to determine the objectives, activities and protective measures to be undertaken. Finally in Finland, an individual welfare plan must be drawn up which identifies the needs of the victim and outlines the operation of appropriate support measures.
- ²⁵⁸ European Parliamentary Research Service (EPRS), op. cit., p. 65
- ²⁵⁹ Bragi Guðbrandsson, Barnahus, “Children’s House: a child-friendly, interdisciplinary and multiagency response to child abuse and services for child victims”, The European Forum on the Rights of the Child, Brussels, 3 -4th of June 2015, http://ec.europa.eu/justice/fundamental-rights/files/rights_child/9th_b_gudbrandsson.pdf; See also, the Children’s Advocacy Center (CAC) model in the US, www.nationalcac.org/multidisciplinary-team/
- ²⁶⁰ Children’s Commissioner for England, “Barnahus: Improving the response to child sexual abuse in England”, www.childrenscommissioner.gov.uk/sites/default/files/publications/Barnahus%20-%20Improving%20the%20response%20to%20child%20sexual%20abuse%20in%20England.pdf
- ²⁶¹ Council of Europe, “Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice”, op. cit., p. 66
- ²⁶² WePROTECT Global Alliance, op. cit., p. 11

- ²⁶³ Lanzarote Convention, Articles 31, 35 and 36; Directive 2011/93/EU, Article 20
- ²⁶⁴ WePROTECT Global Alliance, op. cit., p. 11
- ²⁶⁵ The interview may take place in the children’s house. The “Barnahus” model provides an example of good practice; Missing Children Europe, ECPAT and eNASCO, op. cit., p. 63: In Poland, the Ministry of Justice, in cooperation with the NGO Nobody’s Children Foundation, has established special “blue rooms” victim interviews and has set up a system for certifying the child-friendly rooms. In France, the interview with child victims may be conducted in forensic units within some hospitals. Law enforcement authorities and medical experts work closely to combine the requirements of the investigation with the medical, psychological and social support of victims. Moreover, adapted interview rooms have been established in some police stations of the South-West on the initiative of the NGO “La Mouette”. In Ireland, the interviews can be conducted either in a suitable room at a Garda station, the home of the victim or a relative, a private area in a hospital, a special victim interview suite or any other carefully selected locations where the victim feels comfortable.
- ²⁶⁶ United Nations Office on Drugs and Crime (UNODC), “Justice in Matters involving Child Victims and Witnesses of Crime, Model Law and Related Commentary”, 2009, www.unodc.org/documents/justice-and-prison-reform/Justice_in_matters...pdf
- ²⁶⁷ Council of Europe, “Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice”, October 2011, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804b2cf3>
- ²⁶⁸ For further information, see also, Thorn, “Thorn Sound Practices Guide”, August 2014, www.wearethorn.org/sound-practices-guide-stopping-child-abuse; ITU and UNICEF, op. cit.
- ²⁶⁹ WePROTECT Global Alliance, op. cit., p. 34
- ²⁷⁰ ECPAT International, “Understanding African children’s use of Information and Communication Technologies (ICTs)”, op. cit., p. 9
- ²⁷¹ WePROTECT Global Alliance, op. cit., p. 32
- ²⁷² PhotoDNA, www.microsoft.com/en-us/photodna
- ²⁷³ Thorn, “Spotlight”, www.wearethorn.org/spotlight
- ²⁷⁴ Thorn’s mission is to drive technology innovation to combat the sexual exploitation of children, www.wearethorn.org
- ²⁷⁵ Thorn, “Industry Hash Sharing Platform”, www.wearethorn.org/reporting-child-sexual-abuse-content-shared-hash
- ²⁷⁶ NetClean, www.netclean.com
- ²⁷⁷ Analyze Platform, www.netclean.com/solutions/analyze ; www.griffeye.com/the-platform
- ²⁷⁸ The Technology Coalition, www.technologycoalition.org
- ²⁷⁹ Financial Coalition Against Child Pornography (FCACP), www.missingkids.com/FCACP; www.icmec.org/fcaccp; For further reading: ICMEC, “Internet Merchant Acquisition and Monitoring Sound Practices to Help Reduce the Proliferation of Commercial Child Pornography”, Financial Coalition Against Child Pornography, March 2016, www.icmec.org/wp-content/uploads/2016/03/FCACPInternetMerchantSoundPracticesFinalMarch2016.pdf; ICMEC, “Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation”, May 2017, www.icmec.org/wp-content/uploads/2017/05/ICMEC-FCACPCryptocurrencyPaperFINAL5-17.pdf

- ²⁸⁰ Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with article 49, www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx
- ²⁸¹ www.unicef.org/crc/index_protecting.html
- ²⁸² Osifunke Ekundayo “Does the African Charter on the Rights and Welfare of the Child (ACRWC) only Underlines and Repeats the Convention on the Rights of the Child (CRC)’s Provisions?: Examining the Similarities and the Differences between the ACRWC and the CRC,” *International Journal of Humanities and Social Science*, Vol. 5, No. 7(1), July 2015, p. 143; www.ijhssnet.com/journals/Vol_5_No_7_1_July_2015/17.pdf
- ²⁸³ Status of ratification, <http://indicators.ohchr.org/>: The US signed the CRC in 1995 but have not ratified it.
- ²⁸⁴ Committee on the Rights of the Child (CRC), www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx
- ²⁸⁵ Through resolution 1990/98, www.ohchr.org/Documents/Issues/Children/SR/E-CN4-RES-1990-68.pdf
- ²⁸⁶ By resolution 7/13, http://ap.ohchr.org/documents/E/HRC/resolutions/A_HRC_RES_7_13.pdf; The mandate is also guided by the CRC and the OPSC, www.ohchr.org/EN/Issues/Children/Pages/Mandate.aspx
- ²⁸⁷ Kenya, Morocco, Madagascar and Benin are among the countries visited by the Special Rapporteur in the past 20 years, www.ohchr.org/EN/Issues/Children/Pages/CountryVisits.aspx
- ²⁸⁸ African Charter on the Rights and Welfare of the Child (ACRWC), Adopted by the 26th Ordinary Session of the Assembly of Heads of State and Government of the OAU, Addis Ababa, Ethiopia - July 1990 (in 2001, the OAU legally became the African Union), entered into force Nov. 29, 1999, OAU Doc. CAB/LEG/24.9/49 (1990), www.acerwc.org/download/the-charter-english/?wpdmdl=8410
- ²⁸⁹ ACRWC, www.acerwc.org/the-charter
- ²⁹⁰ ACRWC, Article 21(2)
- ²⁹¹ ACRWC, Article 29(b)
- ²⁹² ACRWC, Article 11(6)
- ²⁹³ ACRWC, Article 26: Protection Against Apartheid and Discrimination
- ²⁹⁴ Also ACRWC, Article 21(1): “*States Parties to the present Charter shall take all appropriate measures to eliminate harmful social and cultural practices affecting the welfare, dignity, normal growth and development of the child...*”
- ²⁹⁵ Morocco is the 55th member State of the African Union. The decision to admit Morocco back into the AU came on January 30, 2017 at the African leaders summit in Addis Ababa, Ethiopia, www.au.int/web/en/memberstates
- ²⁹⁶ The 7 member states which have signed but not yet ratified the Charter are: Democratic Republic of Congo, Morocco, Sahrawi Arab Democratic Republic, Somalia, Sao Tome and Principe, South Sudan and Tunisia, www.acerwc.org/ratification-data; List of countries which have signed, ratified/acceded to the ACRWC, 01/04/2016, www.au.int/web/sites/default/files/treaties/7773-sl-welfare_of_the_child_o.pdf
- ²⁹⁷ ACRWC, Articles 32-46

- ²⁹⁸ ACRWC, Article 42(b)
- ²⁹⁹ ACRWC, Article 43; Reporting Status under the ACERWC, www.acerwc.org/ratification-data: Kenya, Tanzania, Rwanda, Burkina Faso and Niger are among the countries that have submitted both their initial and periodic reports to the ACERWC; Benin, Madagascar, Ethiopia, Uganda, Mali, Togo and Ivory Coast have submitted only their initial report.
- ³⁰⁰ International Labour Organisation (ILO) Convention 182 concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour, adopted by the International Labour Conference, at its 87th Session in Geneva, in June 1999, Date of entry into force: 19 Nov 2000, www.ilo.org/dyn/normlex/en/f?p=1000:12100:0::NO::P12100_ILO_CODE:C182
- ³⁰¹ <http://ilo.org/ipec/Campaignandadvocacy/Youthinaction/C182-Youth-orientated/C182YouthConvention/lang--en/index.htm>
- ³⁰² Ratifications of ILO C182, www.ilo.org/dyn/normlex/en/f?p=1000:11300:0::NO:11300:P11300_INSTRUMENT_ID:312327
- ³⁰³ Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002, www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx
- ³⁰⁴ <http://www.humanium.org/en/childrens-rights-history/references-on-child-rights/protocol-child-sale/>
- ³⁰⁵ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 12
- ³⁰⁶ The countries targeted by this report are among those that have ratified the OPSC, with the exception of Kenya, which has signed but not ratified it to date, <http://indicators.ohchr.org/>
- ³⁰⁷ Convention on Cybercrime, ETS No.185, Budapest, 23/11/2001, Entry into force 01/07/2004, www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
- ³⁰⁸ Council of Europe, “Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime”, Based on a study by Zahid Jamil (Pakistan) for the GLACY+ Project, p. 3, <https://rm.coe.int/16806bfof8>
- ³⁰⁹ Explanatory Report to the Convention on Cybercrime, Paragraph 93, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>
- ³¹⁰ Details of Treaty No.185, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- ³¹¹ United Nations Office on Drugs and Crime (UNODC), “Comprehensive Study on Cybercrime”, Draft, February 2013, p. xix, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- ³¹² Chart of signatures and ratifications of Treaty 185, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=rUztyXH7; Council of Europe, “Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime”, op. cit., p. 3: From the African continent, Mauritius and Senegal have ratified the Budapest Convention, South Africa has signed, while Ghana and Morocco have been invited to accede.
- ³¹³ Council of Europe, “Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime”, op. cit., p. 8
- ³¹⁴ Cybercrime Programme Office of the Council of Europe (C-PROC), www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

- ³¹⁵ GLACY+ is a joint project of the European Union (Instrument Contributing to Peace and Stability) and the Council of Europe, www.coe.int/en/web/cybercrime/glacyplus
- ³¹⁶ www.coe.int/en/web/cybercrime/-/glacy-goes-regional-first-regional-introductory-judicial-training-of-trainers-tot-for-west-african-countries
- ³¹⁷ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.201, Lanzarote, 25/10/2007, Entry into force 01/07/2010, www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084822
- ³¹⁸ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 14
- ³¹⁹ Lanzarote Convention, Preamble: “*Observing that the sexual exploitation and sexual abuse of children have grown to worrying proportions at both national and international level, in particular as regards the increased use by both children and perpetrators of information and communication technologies (ICTs), and that preventing and combating such sexual exploitation and sexual abuse of children require international co-operation;*”
- ³²⁰ See also, “Opinion on Article 23 of the Lanzarote Convention and Its Explanatory Note”, op. cit., Paragraph 20
- ³²¹ The “Lanzarote Committee” (i.e. the Committee of the Parties to the Convention) is the body established to monitor whether Parties effectively implement the Lanzarote Convention. The monitoring procedure is divided by rounds, each round concerning a theme.
- ³²² Lanzarote Committee, “List of decisions 18th meeting”, T-ES(2017)10_en, 6 June 2017, paragraph 4, <https://rm.coe.int/t-es-2017-10-en-list-of-decisions-18th-meeting/168071cb60>; See also, Lanzarote Committee, “Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies (ICTs)”, T-ES(2017)03_en final, 12 May 2017, <https://rm.coe.int/t-es-2017-03-en-final-interpretative-opinion/168071cb4f>
- ³²³ The accession process at the Council of Europe level consists of three steps: (1) Request for accession in an official letter (signed by the Minister of Foreign Affairs or a diplomatic representative) addressed to the Secretary General; (2) Consultation of the Parties to the Convention to obtain their unanimous consent; (3) Decision on the request by the Committee of Ministers, www.coe.int/en/web/children/convention
- ³²⁴ Chart of signatures and ratifications of Treaty 201, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures; Secretariat of the Lanzarote Committee, “Briefing, Information document prepared by the Secretariat of the Lanzarote Committee”, Up-dated on 27 February 2017, <https://rm.coe.int/16806f7d9e>: Morocco’s request to accede to the Convention has been accepted by the Committee of Ministers.
- ³²⁵ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093> (Note that the Directive is wrongly referred to as 2011/92/EU on the Eur-lex website)
- ³²⁶ The Directive 2011/93/EU is included in this study as regional (European) legislation on combating child sexual abuse and exploitation, even if non-EU Member States cannot request accession, because: (1) since it is the most comprehensive legal text on this matter, it could be served as guidance for the elaboration of domestic legislation by other countries worldwide; (2) where child sex tourism takes place outside the European Union, third countries may be called to cooperate –thus facilitate the implementation of the Directive- with EU Member States, through the available national and international instruments including bilateral or multilateral treaties on extradition, mutual assistance or a transfer of the proceedings; (3) cooperation between Member States and non-Member States is essential for the removal of child sexual abuse images from servers in non-Member States.

- ³²⁷ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit., p. 11
- ³²⁸ Directive 2011/93/EU, Recital 12
- ³²⁹ Directive 2011/93/EU, Recitals 46 and 47 and Article 25
- ³³⁰ Brexit: For the time being, the United Kingdom remains a full member of the EU and rights and obligations continue to fully apply in and to the UK, http://europa.eu/european-union/about-eu/countries_en
- ³³¹ National transpositions by Member State, <http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32011L0093>: All EU Member States have transposed the Directive 2011/93/EU except Denmark.
- ³³² African Union Convention on Cyber Security and Personal Data Protection, Adopted by the 23rd Ordinary Session of the Assembly of the Union, held in Malabo, Equatorial Guinea, 27th June 2014, [www.au.int/web/sites/default/files/treaties/29560-treaty-0048 - african union convention on cyber security and personal data protection e.pdf](http://www.au.int/web/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)
- ³³³ Malabo Convention, Preamble
- ³³⁴ Malabo Convention, Article 29(2)(f)
- ³³⁵ Malabo Convention, Article 30(2)
- ³³⁶ Malabo Convention, Article 31(1)
- ³³⁷ Malabo Convention, Article 28
- ³³⁸ www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection: Benin, Chad, Congo, Guinea Bissau, Mauritania, Sao Tome and Principe, Sierra Leone and Zambia have signed the Malabo Convention
- ³³⁹ Date of ratification by Senegal 03/08/2016, at Auguste Yankey, “AU Commission, African Union Convention on Cybersecurity and Personal Data Protection and AU Perspectives on Cybersecurity and Cybercrime Issues”, Octopus Conference 2016, Council of Europe, 17/11/2016, <https://rm.coe.int/16806be017>
- ³⁴⁰ ICMEC, “Child Pornography: Model Legislation & Global Review”, op. cit.
- ³⁴¹ For the purposes of the ICMEC report, mere labor legislation that simply bans the “worst forms of child labor,” among which is child pornography, is not considered “legislation specific to child pornography.”
- ³⁴² Status as of 02/06/2017

