United Nations A/HRC/31/34

General Assembly

Distr.: General
1 December 2015

Original: English

Human Rights Council
Thirty-first session
Agenda items 2 and 3
Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General

Promotion and protection of all human rights, civil political, economic, social and cultural rights, including the right to development

Information and communications technology and child sexual exploitation

Report of the Office of the United Nations High Commissioner for Human Rights

Summary

In the present report, the Office of the United Nations High Commissioner for Human Rights provides an analysis of the legal framework applicable to child sexual exploitation online, and identifies the different forms of sexual exploitation online, including sexual abuse material, grooming, “sextorsion” and child sexual abuse live streaming. It focuses on ways of preventing this phenomenon through legislation and empowerment strategies for children and caregivers, includes examples of good practices and makes recommendations on fighting the sexual exploitation of children online.

I. Introduction

1. The present report is submitted pursuant to Human Rights Council resolution 28/19, in which the Council requested the Office of the United Nations High Commissioner for Human Rights (OHCHR) to prepare a report on the theme of information and communications technology and child sexual exploitation, in close collaboration with the Special Representative of the Secretary-General on Violence against Children and the Special Rapporteur on the sale of children, child prostitution and child pornography, as well as other stakeholders, including States, the United Nations Children's Fund (UNICEF), other relevant United Nations bodies and agencies, relevant special procedures mandate holders, regional organizations and human rights bodies, civil society, national human rights institutions and children themselves, and to present it to the Council at its thirty-first session. The report is also based on recent studies by the relevant mechanisms in this regard, and the need to ensure follow-up to the recommendations contained therein.

II. Current context

2. Information and communications technology (ICT), which encompasses any communication device or application, including radio, television, cellular telephones, and computer and network hardware and software, is no longer an optional add-on to children's lives, but an increasingly integral component of everyday life. It is as important to the educational and social development of children and young people as to the entire global economy. In a recent survey of adolescents in nine countries in Latin America, more than 80 per cent considered quality access to the Internet a fundamental human right (see A/69/264, para. 76).

3. Growing access to the Internet has brought about almost unlimited possibilities for children in their access to content and the exercise of their rights, including the right to receive and impart information and to express opinions. It provides new opportunities for informal and formal education, creativity, social interaction and civic participation. Such benefits nonetheless entail growing risks for children; in particular, the rapid expansion of the Internet globally, with its increasing and instant reach to individuals, has exposed more children and young people to the risk of sexual abuse and to new forms of sexual exploitation. These include the proliferation of child sexual abuse images and materials (child pornography); inappropriate contact with children and "grooming" by unknown adults; the distribution of self-generated content, including "sexting"; sexual coercion ("sextortion") of children; and the broadcasting of videos of the sexual abuse of children, including by live streaming.

4. This rapidly evolving environment makes it difficult for legislators and policymakers to keep up with adequate protection for children. Given the transnational nature of the Internet and the challenges in detection, investigation, victim identification and enforcement that it poses, States, international organizations and the corporate sector need to work together to address them.

5. It is nonetheless important to recall that online risks do not necessarily translate into actual harm to children. When effective strategies are being developed, care should be taken to differentiate between online risks and harm resulting from online activities. It is important to go beyond simply attempts to avoid threats to developing children's capacities as digital citizens and their ability to respond to such challenges. Rather than curtailing children's natural curiosity and sense of innovation for fear of encountering risks online,

efforts should be made to capitalize on their resourcefulness and to strengthen their resilience while exploring the potential of the Internet.[1]

III. International legal framework

6. The Convention on the Rights of the Child does not specifically refer to online protection of children's rights. Indeed, the worldwide web only came online in 1989 (the term "Internet" had been used for the first time only seven years earlier), the same year that the Convention was adopted by the General Assembly.

7. Nonetheless, the Convention on the Rights of the Child and the Optional Protocols thereto, and the Protocol on the sale of children, child prostitution and child pornography in particular, are fully applicable to the digital environment, and provide important guidance for the realization of children's rights online. In particular, the Convention calls for all measures to be guided by the best interests of the child (art. 3), to respect and support children's growing autonomy and agency (art. 12) and to protect children from discrimination and violence (arts. 2 and 19). These articles help to capitalize on the potential of the online environment to promote children's learning and freedom of expression (art. 13), to support children in their access to, receiving and imparting information (arts. 13 and 17), and to protect them from harmful materials and information (art. 19), from unlawful interference with their privacy or correspondence, and from situations where their honour and reputation may be at risk (art. 16).

8. The Convention on the Rights of the Child requires children to be protected against all forms of abuse and neglect (art. 19), including sexual exploitation and sexual abuse (art. 34), and other forms of exploitation prejudicial to the child's welfare (art. 36). With regard to images of child sexual abuse, the Optional Protocol on the sale of children, child prostitution and child pornography prohibits 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, requiring every State to ensure that producing, distributing, disseminating, importing, exporting, offering, selling or possessing child pornography is fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis. The Optional Protocol also requires States to criminalize possession of child pornography with the intent to distribute, disseminate and/or sell it.

9. Article 6 of the Optional Protocol on the sale of children, child prostitution and child pornography calls upon States parties to afford one another the greatest measure of assistance in connection with investigations or criminal or extradition proceedings, including assistance in obtaining evidence at their disposal necessary for the proceedings. Such assistance is particularly important given the global nature of the Internet and the international dimension that characterizes much online violence, exploitation and abuse. In addition, under article 9 of the Optional Protocol, States parties are required to adopt or strengthen, implement and disseminate laws, administrative measures, and social policies and programmes to prevent the offences to which it refers. Paying special attention to especially vulnerable children is another concern expressed, as well as awareness in the public at large, including children, through information by all appropriate means, education and training, about the preventive measures and harmful effects of the offences referred to

[1] 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. 22.

in the Optional Protocol. Article 9 also addresses the important issue of rehabilitation and compensation for children who have fallen victim to offences involving images of child sexual abuse.

10. In recent years, the Committee on the Rights of the Child has given increasing attention to ICT and the Internet in its concluding observations. In its recommendations, the Committee has highlighted crucial areas requiring further efforts, including the adoption of a national coordinating framework to address all forms of violence against children, including on the Internet (CRC/C/LUX/CO/3-4, para. 30 (b)); the passing of comprehensive legislation to criminalize “all forms of child pornography and sexual exploitation of children on the Internet” (CRC/C/CHN/CO/3-4, para. 46 (d)) and the solicitation of children for sexual purposes and accessing child pornography by means of ICT (CRC/C/OPSC/PRT/CO/1, para. 26 (a)); measures to prevent the publication and dissemination of pornographic material concerning children through surveillance mechanisms to automatically block offending Internet service providers and other media; taking prompt steps to establish an authority for Internet safety, licensing of service providers and checks for content harmful to children (see CRC/C/OPSC/USA/CO/2); and encouraging cooperation with ICT and other relevant industries to facilitate the development of voluntary, self-regulatory, professional and ethical guidelines and standards of conduct and other initiatives, such as technical solutions promoting online safety that are accessible to children (CRC/C/CHE/CO/2-4, para. 37 (b)). It has also considered the significant impact that digital media and ICT are having on children’s lives; its general comments No. 13 (freedom from all forms of violence), No. 14 (best interests), No. 16 (business sector) and No. 17 (right to rest, leisure and play) all make explicit reference to digital media and ICT. Furthermore, in 2014, its day of general discussion was focused on the theme of “digital media and children’s rights”.

11. Other bodies have adopted international standards to combat cybercrime and protect children from online risks and harm, including the United Nations Convention against Transnational Organized Crime and Convention No. 182 of the International Labour Organization on the Worst Forms of Child Labour.

12. Several regional conventions are applicable to the issue of child sexual exploitation online, including the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and the Convention on Cybercrime; the African Union Convention on Cyber Security and Personal Data Protection; the Agreement on Cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information; and the Arab Convention on Combating Information Technology Offences.

IV. Identifying child sexual exploitation online

A. Scope of the problem

13. At the beginning of 1998, fewer than 200 million people around the world were online. The International Telecommunication Union (ITU) estimates that, by the end of 2015, the number of Internet users globally will have reached 3.2 billion. Of these, two

thirds live in the developing world, where the number of Internet users has doubled in five years, from 974 million in 2009 to 1.9 billion in 2014.[2]

14. The growth in connectivity has been accompanied by changes in the way in which users access the Internet. The penetration of sophisticated mobile technology means that many online activities are no longer being conducted via computers in fixed locations. When children use mobile technology, it becomes more difficult for parents or caregivers to monitor their online activity or to restrict, monitor or control what they access.[3] Furthermore, the growing population of children using the Internet opens up opportunities for perpetrators to connect with potential victims online. The greater availability of inexpensive mobile devices facilitates the production of child sexual abuse material, while the emergence of broadband has helped to facilitate the exchange of child sexual abuse materials, including files containing photographs, video and audio. Lastly, an increasing number of encryption tools and platforms afford different levels of anonymity to online child sex offenders, making it harder for the authorities to detect illegal conduct and to identify perpetrators online.

15. While the growth of the Internet has not in itself created the risk to children, it is increasingly one of the places where problems now arise. The opportunities that the Internet affords may amplify, complicate or heighten the potential impact of existing and evolving forms of violence, abuse and exploitation.

B. Forms of sexual exploitation online

1. Sexual abuse material

16. The creation, publication and distribution of child sexual abuse material online are among the activities facilitated by new technologies that capture the most attention. Article 3 (1)(c) of the Optional Protocol on the sale of children, child prostitution and child pornography requires States to criminalize the production, distribution, dissemination, import, export, offer, sale or possession of child pornography. New technologies have, however, transformed what is actually intended by "possession", given that the growth in Internet speed has made it no longer necessary to download and store images because they can be viewed online.

17. The scale of child abuse material on the Internet has reached an unprecedented level, with many individual offenders in possession of millions of such images and/or videos. There has also been a shift in the way material is traded, moving away from commercial sites to peer-to-peer networks, which facilitate evading filtering and other detection software and therefore reduce the risk of detection of those seeking and distributing child pornography (E/CN.15/2011/2, para. 15). Law enforcement operations against peer-to-peer sharing of files containing child sexual abuse images have identified millions of Internet protocol addresses offering child pornography.[4] Also, the use of "cloud" services guarantees a degree of user anonymity when exchanging and storing child sexual abuse online, without any need to host these materials on personal devices. Furthermore, online virtual currencies are sometimes used to pay for child sexual abuse materials. Such currencies are often subject to less transparency, and allow users to evade measures taken

[2] See ITU Facts and Figures: The World in 2015, available at www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

[3] UNICEF, Child Safety Online: Global challenges and strategies, December 2011, p. 4.

[4] United States Department of Justice, "The National Strategy for Child Exploitation Prevention and Interdiction", August 2010.

by the financial industry to combat commercial exploitation (A/HRC/28/56, para.28). In addition, financial transactions are more difficult to trace in the context of criminal investigations.

18. According to one non-governmental organization, , online child sexual exploitation is likely to rise in coming years as Internet adoption rates expand globally and demand increases for new child sexual abuse material. The organization and its member hotlines reported a 14 per cent increase in the number of complaints concerning illegal online content handled globally in 2013, and a 47 per cent increase in the number of confirmed reports of child sexual abuse material.[5]

19. Young victims are often the target of these practices. According to the United Nations Office on Drugs and Crime, between 2011 and 2012 there was a 70 per cent increase in child sexual abuse material focused on girls under the age of 10 years, and abuse material involving toddlers or babies is not uncommon (A/HRC/28/55, para. 59). The majority of victims are female: 81 per cent of the children depicted in known child abuse material are girls.[6] Once online, child abuse images can circulate indefinitely, perpetuating the harm to children. The circulation of such images contributes to the promotion of a subculture in which children are perceived as sexual objects, and also strengthens the belief among those who belong to those communities that it is a “normal” practice since so many others share the same taste for children (A/69/264, para. 96).

2. Grooming

20. One form of exploitation and abuse that is not expressly mentioned in the Optional Protocol to the Convention on the Rights of the Child is the solicitation of children, also referred to as “grooming”. This is not a new form of exploitation, since grooming – which involves conditioning the child to ensure that he or she acquiesces to sexual contact – has long been a part of the process of abusing a child. The Internet can, however, accelerate the grooming process (A/HRC/28/56, para. 38) and allow its reach to be internationalized in ways that were previously impossible. The advent of social media has further enabled child exploiters to more readily engage in grooming by using social media platforms to connect with child victims. According to UNICEF, the Internet deconstructs traditional boundaries of privacy by creating situations in which children engage in conversation in apparently private settings, while in fact exposing themselves, wittingly or unwittingly, to an unknown, worldwide audience. The warning signs that can serve to protect children in the physical world, such as physical and behavioural cues, or the appraisal of friends or caregivers – are largely absent online.[7]

21. While initial concerns focused on offenders who sought to meet children offline, behaviour has changed to include other manifestations. It is increasingly common for solicitation to consist of persuading the child to engage in sexual activity in front of a webcam, the footage of which will then be recorded or to send sexualized photographs to the offender. Once the footage or photographs have been gathered, often the child will be subjected to threats if she or he refuses to produce similar material or to pay money (A/HRC/28/56, para. 38).

[5] International Association of Internet Hotlines (INHOPE), “Online child sexual exploitation likely to rise in the coming years”, 16 April 2014.

[6] See INHOPE, victim profiles, at www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx.

[7] UNICEF, Child Safety Online (see footnote 3), p. 5.

22. Determining the frequency of grooming is problematic owing to the reluctance of many victims to report abuse. Some studies suggest, however, that almost one in three children in Europe aged between 9 to 16 have communicated with someone they did not know online;[8] in Latin America, as many as 40 per cent had done so.[9] While it is possible that not all contacts are harmful, it has been estimated that between 13 and 19 per cent of children have experienced unwanted sexual solicitation.[10]

23. It should be emphasized that publicity concerning online predators attempting to lure children into sexual relations by lying about their age misrepresents the overall picture and nature of the problem. Studies suggest that Internet sex crimes are more likely to fit a model of statutory rape involving adult offenders who openly seduce underage teenagers rather than a process of forced sexual assault, age deception or paedophilic child abuse.[11] Research conducted in the United States of America suggests that most online offenders are, in fact, open about being older adults.[12] Such openness may potentially complicate initiatives to protect adolescents from this kind of contact risk given that they may not regard themselves as victims.

3. Circulation of self-generated content

24. While many sexual images of children are created and distributed without their consent or knowledge, other images with sexual content may be produced by the children themselves. The creation and distribution of child-generated sexual content as a part of "intimate" online interaction or as a result of peer pressure is now a widespread phenomenon. Often referred to as "sexting", there is a real risk that the material will be viewed by persons for whom it was not intended. One study found that 89.9 per cent of the images assessed had been harvested from the original upload location and were being redistributed on third-party websites.[13]

25. In 2013, a survey conducted by ChildLine, a non-governmental organization, of teenagers aged between 13 and 18 years in the United Kingdom of Great Britain and Northern Ireland found that 60 per cent of participants had been asked for a sexual image or video of themselves; 40 per cent replied that they had created an image or video of themselves; and 25 per cent stated that they had sent an image or video of themselves to someone else. While most stated that the image had been sent to a boyfriend or a girlfriend, one third had sent it to someone they had met online but did not know in real life, while 15 per cent had sent it to a total stranger.

26. It is important to work with children to raise their awareness of the risks involved in this practice. It is furthermore necessary to ensure that any problem can be adequately addressed as soon as it arises. Firstly, children should have access to a child-friendly reporting and complaint mechanism that provides a secure and confidential way of

[8] Stephen Webster et al., European Online Grooming Project: Final Report, European Commission, March 2012, pp. 24–25.

[9] Sergio García de Diego, *Understanding the use of ICTs by children and young people in relation to their risks and vulnerabilities online specific to sexual exploitation: a youth-led study in Latin America* (ECPAT International, Bangkok, June 2012), p. 38.

[10] Helen Whittle et al., "A review of young people's vulnerabilities to online grooming", *Aggression and Violent Behaviour*, vol. 18, No. 1 (January–February 2013), p. 65.

[11] UNICEF, Child Safety Online (see footnote 3), p. 40.

[12] Janis Wolak, "Research findings in the United States about sexual exploitation via virtual interactions", in *Research Findings on Child Abuse Images and Sexual Exploitation of Children Online* (ECPAT International, Bangkok, 2009), p. 7.

[13] Internet Watch Foundation, Emerging Patterns and Trends Report #1: Youth-Produced Sexual Content, 10 March 2015.

reporting self-generated sexually explicit content to the relevant authority. Secondly, once it has been confirmed that an image or video of a child is of a sexually explicit nature, procedures must exist to ensure fast and effective removal of the content.

4. Sexual extortion or “sextortion”

27. Self-generated images are sometimes used by perpetrators to manipulate or coerce children to obtain sexual favours from them. “Sextortion” refers to the process by which a person is coerced with a view to procure sexual favours, sexual material, money or other goods. There usually is a perceived imbalance of power between the perpetrator and the victim allowing the perpetrator to exert coercive pressure on the victim to accede to sexual or monetary demands. The sexual component in this practice can involve demands for all types of sexual activity, such as exposing private body parts, posing for sexual photographs or submitting to physical abuse.

28. Many young people and children sharing self-generated sexual content online do not take any steps to conceal their identity or location. This increases the risk of extortion by perpetrators using identifying information and personal information to coerce the victim. In additionally, when the extortion results in the dissemination of self-generated indecent images online, this can result in other negative consequences for the victims, such as cyberbullying, further victimizing the child.

5. Child sexual abuse live streaming

29. In recent years, rising Internet coverage, the availability of improved broadband connections and mobile technology combined with other social and cultural factors in the developing world have facilitated the emergence of an evolving form of child online sexual exploitation: child sexual abuse live streaming.[14] In this case, adults pay to direct and view a live video of children performing sexual acts in front of a webcam. The practice transcends borders, given that the viewer may be located in any part of the world without the need to travel, which makes detection and enforcement more difficult.

C. Risk factors increasing vulnerability

30. While Internet coverage is spreading rapidly across the globe, its development is not equal, with online connectivity varying greatly from one country to another. Moreover, children may interact with the Internet in different ways, which makes them vulnerable to different risks.

31. In poorer countries, children who have access to the Internet may be particularly vulnerable to online solicitation because their economic situation may pressure them into accepting propositions that include payment.[15] At the same time, parents and teachers might be unaware of the online risks involved, effectively removing an important source of support and protection for children.

32. Different age groups experience online risks in different ways and are also targeted differently. Younger children may be particularly vulnerable online because they lack technical expertise and the ability to identify possible risks. According to figures compiled by the Internet Watch Foundation, more than 80 per cent of victims in known child sexual

[14] See Save the Children, “Webcam Child Sex Tourism. Becoming Sweetie: a novel approach to stopping the global rise of Webcam Child Sex Tourism”.

[15] Warren J. Blumenfeld and R.M. Cooper, “LGBT and Allied Youth Responses to Cyberbullying: Policy implications”, *International Journal of Critical Pedagogy*, vol. 3, No. 1, 2010.

abuse images are 10 years of age or younger (while 3 per cent are 2 years of age or younger). This figure is up from 74 per cent in 2011.[16] On the other hand, older children are the primary targets of sex offenders who use the Internet to groom victims and to meet them offline,[17] and may also face unusually high risks of exposure to harmful material and cyberbullying (E/CN.15/2014/7, para. 40).

33. Gender differences also influence how children perceive and respond to online risk: while boys appear to be more bothered by online violence than girls, girls are more likely to be concerned by contact-related risks.[18]

34. Research suggests that young people who already face challenges in their daily lives are also at risk of encountering problems online. Children belonging to vulnerable groups − including those of lower socioeconomic status, children affected by migration, children out of school, children belonging to minorities and children with disabilities − may be less likely to enjoy the benefits offered by the online environment or to receive information regarding online safety than their peers.[19]

35. Social isolation also affects the nature of a child's online behaviour and the amount of activity online, as well as a child's propensity to seek help when problems arise (E/CN.15/2014/7, para. 40). Isolated children and adolescents are more likely to share sensitive information publicly, including inappropriate or sexually explicit material, with a view to gaining acceptance and attention (ibid., para. 29). This has led researchers to identify a "double jeopardy" effect whereby children with more psychological problems suffer greater harm from both online and offline risks.[20]

V. Preventing and addressing child sexual abuse and exploitation through information communications technology and the Internet

36. The challenge of creating a safe online environment for children lies in developing a range of responses that strike a balance between maximizing the potential of ICT to promote and protect children's rights while minimizing risks and ensuring children's safety and protection. A digital agenda for children should be integrated as a core component of a comprehensive national, coordinated and well-resourced policy framework to prevent and address all forms of violence against children. To be effective, the agenda should be inclusive and empowering, involve all stakeholders, aim at reaching all children, and be informed by their views and experiences online.

37. The main components of such a strategy include legislative reform; developing policy and guidance for relevant sectors; strengthening institutions; achieving better coordination through multi-stakeholder engagement; capacity-building; and systematic data collection and research.

[16] See E/CN.15/2014/CRP.1, para. 126.

[17] Janis Wolak, "Research findings in the United States about sexual exploitation via virtual interactions" (see footnote 12), pp. 6-9.

[18] Sonia Livingstone et al., Risks and safety on the internet: the perspective of European children, LSE Research Online, 2011, p. 62.

[19] Special Representative of the Secretary-General on Violence against Children, *Releasing Children's Potential and Minimizing* Risks (see footnote 1), p. 18.

[20] Leen d'Haenens, Sofie Vandoninck and Verónica Donoso, "How to cope and build online resilience?", EU Kids Online, 2013, p. 1.

A. Prohibition, criminalization, prosecution and the victim’s right to effective assistance and redress

1. National legislation

38. Many States do not have an adequate legislative framework to facilitate effective investigations into and prosecution of online sexual exploitation and abuse of children. In 2012, only 69 of 196 States had legislation considered sufficient to combat child pornography offences, while 53 States still had no legislation that specifically addressed child pornography. Of the 74 States that had some legislation specifically addressing child pornography, 47 did not criminalize the knowing possession of child pornography, regardless of intent to distribute.[21] Equally, criminal procedure and evidence laws do not reflect the unique challenges of investigating and prosecuting offences related to online sexual exploitation and abuse of children.

39. National legislation is indispensable if children’s access to ICT and the enjoyment of digital literacy without discrimination of any kind are to be assured. The law should ban all forms of violence in all settings, including cyberspace; secure children’s protection; provide for effective remedies, recovery and reintegration to address online harm, abuse or exploitation; and establish child-sensitive counselling, reporting and complaint mechanisms and procedures, as well as mechanisms to fight impunity.

40. Although legislation must be flexible in order to avoid constant updating, it must convey a clear message of prohibition of all manifestations of violence. It should address loopholes associated with emerging concerns, including new forms of online abuse, and develop procedures in criminal proceedings to facilitate investigation and prosecution. In addition, legislation should apply extraterritoriality, and prohibit abuse of children wherever in may occur.

2. Detection and reporting

41. Given the global nature of child online sexual abuse, it is important that States strengthen cooperation through multilateral, regional and bilateral arrangements. Mutual legal assistance and transnational cooperation for effective detection and reporting systems, information-sharing and other security systems are crucial. Under the Optional Protocol on the sale of children, child prostitution and child pornography, States are required to cooperate in the investigation, extradition or criminal proceedings brought in respect of the abuse or exploitation of children. Extraterritorial jurisdiction for those crimes could have a deterrent effect, but requires effective international cooperation.

42. International cooperation should be complemented by partnerships with other stakeholders, particularly the private sector, to develop the technological tools necessary to enable identification, investigation and prosecution before the courts, as well as the active involvement and participation of children as advocates of child protection. Governments should establish accessible, safe and child-friendly reporting systems and institutions, which should be supported by effective and well-resourced services, and respectful of children’s rights.

43. Research suggests that reporting tools offer a particular benefit to girls, vulnerable children and children from poorer homes, and that the more widely and deeply children use the Internet, the more likely they are to use reporting tools if upset by something they

[21] See International Centre for Missing & Exploited Children, *Child Pornography: Model Legislation & Global Review*, 7th ed. (Alexandria, Virginia, 2013), p. iv.

encounter online. Children less experienced in Internet use should therefore be specifically encouraged and enabled to use online reporting tools, which should be easy to use and simple.[22]

3. Blocking and filtering

44. Blocking and filtering lists are important mechanisms used to combat child sexual abuse and exploitation online, by preventing such content from being accessed. It does not in and of itself constitute censorship or a violation of the right to freedom of opinion and expression; as noted by the Special Rapporteur on freedom of opinion and expression, however, child protection concerns have been used as a cover for inappropriate or disproportionate blocking and filtering on issues such as sexual and reproductive health, sexuality, politics and advocacy (A/HRC/17/27, para. 9).

45. States should establish clear rules to prevent filtering and blocking systems from being used to process anything other than child sexual abuse material. Blocking lists and filtering should have a clear legal basis, sufficient transparency and effective safeguards against misuse, including judicial oversight. All citizens, and especially children, should have the right to know about any restrictions that are in place, and have the basis for them explained.

4. Training of law enforcement and those involved in the administration of justice

46. In conjunction with a strong legislative framework, it is also important that specialist law enforcement units be created to investigate those offences and that they work closely with specialist agencies that are trained to work with child victims. These investigations require highly sophisticated, cutting-edge technology, such as forensic computer analysis, to gather the appropriate electronic evidence. Law enforcement online is particularly challenging given that physical contact need not occur in order for a crime to be committed, and much of the evidence involved in these cases is in a volatile electronic format that may elude traditional policing methods.[23] Only by building up a framework of dedicated officers can those offences be properly tackled (A/HRC/28/56, para. 54).

47. In addition to specialized forces, it is important that training on offences relating to sexual abuse of children be institutionalized in the training for all members of the judiciary, prosecutors and law enforcement. This is required to handle digital evidence and to assess the weight and value of this type of evidence, as well as to understand child abuse and exploitation cases associated with the use of new technologies.

5. Care, recovery and reparation for victims

48. When considering the detection, investigation and prosecution of child online sexual exploitation, it is important that the process be victim-centred. Recovery of the child and the avoidance of re-victimization should be given due consideration when deciding whether and when to prosecute an offender. In the best interest of the child, that may entail allowing the victim a period of recovery to receive the necessary support, as well as assistance in cases where the child victims will interact with the justice system. Criminal prosecution of a perpetrator should not adversely affect the health and recovery of the victim, and the victim’s rights and interests should be secured and protected throughout the legal process.

[22] Special Representative of the Secretary-General on Violence against Children, *Releasing Children’s Potential and Minimizing* Risks (see footnote 1), p. 59.

[23] UNODC, Comprehensive Study on Cybercrime, February 2013, p. xi.

49. While the majority of international law is focused on the criminalization of activities and the punishment of offenders, there should also be recognition of the need to provide redress to child victims and to compensate them for the harm suffered. Compensation and restitution measures may ensure that child victims have the means to seek rehabilitation, recovery and reintegration. The ability to bring civil action should be provided regardless of the economic status of the victim, including through the provision of legal aid or through the establishment of a State-operated compensation system.

B. Empowerment of children

50. Giving children the tools to protect themselves against threats on the Internet and to become more aware of their responsibilities is one of the most effective ways of safeguarding children's rights not to be sexually exploited and abused. Children adopt new technologies with ease, but they need skills and confidence to be able to feel secure when they explore the borders of the digital universe. Children need to develop their capacities as digital citizens.

51. At the same time, children should be encouraged to develop their social skills and their "social literacy". Digital and social literacy skills provide the foundation for the responsible use of ICT, and can enhance a child's capacity to protect him or herself from harm. In particular, children with both digital and social skills are more likely to avoid, and adequately respond to, risks that they may encounter in the digital world.[24]

52. A degree of risk is inherent in the use of ICT, with risk not just deriving from children's behaviour online but also from the behaviour of others (such as peers) and perpetrators online and offline; the risk does not, however, inevitably translate into harm for children and young people. The more children engage in online activities, the more they gain skills and resilience, and become self-confident. In turn, the more skills they possess, the more opportunities they may explore, with a greater chance of encountering associated risks. More skills can, however, reduce the harm that children experience, and help children to cope better with such risks.

53. The potential of children to address their own protection concerns is closely associated with their evolving capacities. The fact that some children and young people adopt new technology quickly does not mean they do not require support, information and guidance on protection strategies in order to remain safe.

54. Given that curiosity is normal and healthy, adolescents need information about the risks and dangers of online contact, in particular with adults. Children should be informed in an age-appropriate and child-friendly manner on how to report threatening or inappropriate interactions and violence, and the process that is likely to follow. This requires the establishment of counselling, complaint and reporting mechanisms that are widely available, easily accessible, child-sensitive and confidential.[25]

55. In accordance with their obligations under article 12 of the Convention on the Rights of the Child, States should ensure the effective and ethical participation of children and young people in the development of policies and practices related to ICT and child sexual exploitation when designing prevention tools and in relation to children's service needs.

[24] Committee on the Rights of the Child, report of the 2014 day of general discussion, "Digital media and children's rights", p. 83.

[25] Special Representative of the Secretary-General on Violence against Children, *Releasing Children's Potential and Minimizing* Risks (see footnote 1), p. 45.

C. Support for families, teachers and caregivers

56. Openness and accessibility are two of the primary advantages of the Internet, but they also entail some of its greatest risks. ICTs, and the unsupervised online access they facilitate, make children potentially vulnerable to violence, abuse and exploitation in ways that are often difficult for parents, caregivers, teachers and others to detect and address.

57. Often even very young children have a more sophisticated understanding of the Internet and mobile phone technologies than their parents and caregivers do. Many parents, teachers and caregivers are therefore not sufficiently informed about online safety tools or on possible online risks for children.

58. While research is still limited in many countries, studies suggest that where parents and teachers have less training and support in Internet use, children engage in more risky behaviours online.[26] Evidence suggests that children are more likely to report unwanted or upsetting contacts or content to parents who themselves understand the Internet or who have been available and open to discussions of Internet use with the child.[27] Parents and caregivers themselves must therefore be supported to better understand the online environment, how children and young people operate in it, the type of risks they might encounter, the harm that can potentially ensue and the most effective ways to avoid this harm and to develop resilience among children and young people.

59. Similarly, communities at large need to be aware of the issue of sexual exploitation online and capable of providing a safe environment for children, as well as a proper response to victims. For children to be able to speak out about this issue, it is necessary to break taboos and eliminate harmful cultural or contextual beliefs that allow exploitation or cause people to keep silent about child sexual exploitation.

60. Schools also have a unique potential to promote non-violent behaviour and to support change of attitudes that condone violence. Through quality education, children can gain the skills and abilities to use the Internet with confidence, to avoid and address risks, and to become well-informed, responsible digital citizens. Education includes promoting creative, critical and safe use of the Internet and preventing and responding to incidents of online violence. A precondition for any school-based initiative is for teachers themselves to understand the online environment and to have the ability to identify early signals of abuse, as well as to advise, guide, empower and support children and young people.[28]

D. Role of the private sector

61. The private sector, an essential driver for societies and economies, can contribute actively to the promotion of children’s rights, minimizing risks and securing online protection for children. While the Internet is used by everyone, it is privately owned. Governments should work together with such actors as Internet service, hosting and content providers, search engines, payment services, telecommunications companies, manufacturers of ICT, “cloud” computing companies, social media sites and even small businesses, such as Internet cafes.

[26] Sonia Livingstone and Monica E. Bulger, *A Global Agenda for Children’s Rights in the Digital Age,* September 2013, p. 21.

[27] Ibid., p. 20.

[28] Special Representative of the Secretary-General on Violence against Children, *Releasing Children’s Potential and Minimizing* Risks (see footnote 1), p. 48.

62. The Guiding Principles on Business and Human Rights, the Children's Rights and Business Principles, and general comment No. 16 of the Committee on the Rights of the Child on State obligations regarding the impact of business on children's rights (CRC/C/GC/16) provide important guidance in this area, addressing the safety of children and preventing the risk of harm, abuse or exploitation. The ITU/UNICEF Guidelines for Industry on Child Online Protection provide a sound framework for promoting the positive use of the Internet and mechanisms for reporting child sexual abuse online, and for encouraging safe and age-appropriate awareness and education for children, parents and teachers (A/69/264, para. 118).

63. While many positive initiatives have been launched and vital tools have been developed, more consistent action is needed, including on restricting access to child sexual abuse material and content harmful to children, age verification and guidance on child safety addressed to children and parents (A/69/264, para. 119). Companies should implement codes of practice and safeguarding standards, and be fully aware of how their services can have an impact on children online and create potential safety risks.

E. International cooperation

64. Given the nature of child sexual exploitation through ICTs, international cooperation is indispensable when tackling the problem. The need for such cooperation is clearly spelled out in both international and regional instruments, and should include cooperation between States, international and regional organizations, and national and international non-governmental organizations.

65. The Special Representative of the Secretary-General on Violence against Children organizes an annual round-table discussion with regional organizations and institutions to enhance cross-regional cooperation and accelerate progress in children's freedom from violence. The forum has become a strategic mechanism in the promotion of policy dialogue, the sharing of knowledge and good practices, facilitating cross-fertilization, coordinating efforts and fostering synergies, identifying trends and pressing challenges, and joining forces to strengthen children's safety and protection.

F. Data collection and further research

66. One of the most significant challenges to understanding children's use of ICTs and engagement with the Internet is the lack of research from developing countries. In many countries, particularly in parts of Asia, the Middle East, and Africa, it is not known whether and how children access the Internet, let alone what the consequences might be (A/69/264, para. 23). These countries are both home to the majority of the world's children and young people and the places where Internet access is now growing most rapidly.

67. Data and research on children's safety, exposure to risk, the impact of harm and factors that affect children's resilience are essential for the development of law and policy. States should undertake research, data collection and analysis on an ongoing basis to gain a better understanding of how children access and use digital and social media, and their impact on children's lives. The data should cover both risks and opportunities for children, and be disaggregated in order to facilitate analysis on the situation of all children, particularly those in a situation of vulnerability.

VI. Examples of good practice

68. The ITU “Connect a School, Connect a Community” initiative is a public-private partnership designed to promote broadband Internet connectivity for schools in developing countries. It is based on the concept that connected schools should cater not only for the children who attend them, but also for the broader communities in which the children live. In this way, schools can serve as community ICT centres for disadvantaged and vulnerable groups, including women and girls, indigenous peoples and persons with disabilities. Children and adolescents attending connected schools will have improved access to the latest ICT, while community members will receive ICT-based training on basic life skills together with training to develop business and ICT-specialized skills.[29]

69. In Costa Rica, a range of legal and policy steps have been taken to enhance children’s online protection. In December 2010, a national commission on online safety was established with a multidisciplinary, inter-sectoral structure, comprising representatives of both public and private institutions. Its role is to devise policies on the safe use of the Internet and ICT, as well as to develop a national plan of online safety. Its activities include raising awareness of the appropriate use of the Internet and digital technologies; proposing initiatives to prevent access by children to inappropriate content; promoting safe access to the Internet; developing strategies to avoid the inappropriate use of the Internet; and proposing legislation to strengthen the rights of individuals, communities and institutions with regard to Internet access.[30]

70. Safer Internet Day is an annual event when countries around the world raise awareness about online safety. Schools are normally involved in the awareness-raising activity to ensure that the message reaches different stakeholders, including children, parents and teachers (A/HRC/28/56, para. 61).

71. INHOPE is a network of 51 hotlines in 45 countries that receives reports of child pornography hosted on the Internet, refers them to the relevant authorities. In 2013, INHOPE received more than 1.2 million reports of illegal content and identified nearly 40,000 unique images hosted on the Internet (A/HRC/28/56, para. 51).

72. The Virtual Global Taskforce is a key example of international cooperation. It consists of 12 law enforcement partners and a number of private sector partners, including Blackberry, Microsoft and PayPal, and a variety of child protection agencies. The Taskforce helps to share intelligence and coordinate law enforcement, which has resulted in successful investigations (A/HRC/28/56, para. 71).

73. The Philippines Anti-Child Pornography Act comprehensively prohibits the creation, distribution and viewing of child pornography. The law requires private sector actors, such as Internet service providers, private business establishments and Internet content hosts, to assist in the fight against child pornography and to notify authorities in the event that they discover that their servers or facilities have or are being used to commit child pornography offences. Service providers are also required to install programmes or software designed to filter and block child pornography. Importantly, the Act requires appropriate forms of protection for child victims of pornography offences, which includes strict confidentiality in the handling of evidence, protecting witnesses and assisting in recovery and reintegration (see A/HRC/28/55).

[29] Special Representative of the Secretary General on Violence against Children, *Releasing Children’s Potential and Minimizing Risks* (see footnote 1), p. 49.

[30] Ibid., p. 57.

74. The Child Helpline International Foundation is a global network of 192 child helplines in 145 countries that together receive more than 14 million contacts a year from children and young people in need of care and protection. It 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 to advocate for the rights of children.

VII. Conclusion and recommendations

75. **While OHCHR notes that efforts have been made at different levels to ensure effective laws and policies to protect children from sexual exploitation online, it is fundamental that States:**

(a) Ratify all relevant regional and international instruments regarding the sale and sexual exploitation of children online;

(b) Establish clear and comprehensive legal frameworks to prohibit and to criminalize all forms of sale and sexual exploitation of children online;

(c) Improve coordination through effective multi-stakeholder engagement bringing together relevant State agencies, non-governmental organizations and representatives of industry; at a general level, a multi-stakeholder platform should be put in place to propose a safe, inclusive and empowering digital agenda for children;

(d) Strengthen support for services responsible for the identification of victims, as well as for the detection, investigation, prosecution and punishment of those responsible for any offences committed;

(e) Ensure that children – both girls and boys, as well as children in vulnerable or marginalized situations – are consulted in order to take into account their views and experiences in developing laws, policies and programmes relating to digital media and ICTs;

(f) Promote and facilitate international and regional coordination and collaboration to ensure effective enforcement of the applicable legal framework;

(g) Establish a permanent global task force to harmonize practices and procedures, share expertise and scale-up good practices, and to provide States with assistance in developing national laws, policies and strategies to effectively combat online child sexual exploitation;

(h) Encourage public-private partnerships to promote the use of ICT to support children's access to information on their rights and to facilitate their participation in the shaping of policies, programmes and services concerning them;

(i) Coordinate with the ICT industry so that it develops and puts in place adequate measures to protect children from the risks posed by ICT. Where such risks are detected, States and industry should work together to provide prompt and effective procedures for the removal of prejudicial or harmful material involving children. States should comply with the ITU/UNICEF Guidelines for Industry on Child Online Protection;

(j) Further strengthen awareness-raising and education programmes for children on preventing and responding to risks when they use digital media and ICT, with the involvement of children, including through the development of child-friendly information material; this should include programmes on privacy risks related to the use of digital media and ICT and regarding self-generated content;

(k) Promote action to empower educators and parents to accompany and support children in acquiring skills to live in the digital environment;

(l) Provide adequate and continuous training for law enforcement personnel, members of the judiciary and professionals working with and for children with the aim to enhance their technical skills;

(m) Ensure accessible, safe, confidential, age-appropriate, child-friendly and effective reporting channels, such as child helplines, for reporting violations of children's rights in relation to digital media and ICT; this should include the provision of safe, child-friendly and confidential points of contact for children to report self-generated sexual content to the relevant authority;

(n) Strengthen coordination between all actors and sectors in the protection system ensuring referral of cases and effective support to children victims; this should include the development of a child protection strategy that ensures that the protection and care of victims is paramount in investigations and that sets out good practices in the handling of victims;

(o) Empower and provide adequate resources to national institutions responsible for guaranteeing human rights to allow them to play a key role in monitoring child online sexual exploitation; such institutions should have a specific mandate to address the rights of children in relation to digital media and ICT, and be able to receive, investigate and address complaints by children in a child-sensitive manner, ensure the privacy and protection of victims, and undertake monitoring, follow-up and verification activities for child victims;

(p) Conduct action-oriented research into the perpetrators of online abuse, the ways in which children are victimized online, and the factors that make individuals more vulnerable, with a view to prevent abuse and strengthen professional responses to victims in terms of investigation, rescue, recovery and reintegration.