
PROTECTING CHILDREN IN CYBERSPACE: AN INTERDISCIPLINARY STUDY OF ONLINE CHILD SEXUAL EXPLOITATION

Anjali, Department of Law, Maharishi Markandeshwar (Deemed to be University),
Mullana, Ambala, Haryana, India

Akanksha, Department of Law, M.M.H. College, Ghaziabad, Uttar Pradesh, India

ABSTRACT

The suddenly growing digital technologies have had a major effect on the way children obtain access to education, communication and socialization and at the same time have afflicted them with unfamiliar digitally based forms of abuse and exploitation. Online Child Sexual Exploitation (OCSE) has become a significant international issue, including: online grooming, Child Sexual Abuse Material (CSAM), sextortion, live-streamed sexual abuse and technology-enabled exploitation. The growing number of social media, online gaming sites, encrypted communications and artificial intelligence has made these crimes even harder to deal with and a major problem for law enforcement agencies and even policymakers.

This paper will take an interdisciplinary perspective in the analysis of the legal, technological, and policy aspects of child sexual exploitation in the online space in India. It examines the constitutional provisions and law enforcement, such as the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023. The position of the recent technology in facilitating as well as combating online exploitation is also an issue of discussion in the study, which outlines the significance of the digital forensics, artificial intelligence, platform responsibility, and international collaboration.

The paper has highlighted some of these obstacles as technological anonymity, encrypted communication, transnational cybercrime, under-reporting offenses, poor digital literacy, and poor institutional coordination. It proposes that legal provisions cannot be alone to take care of the dynamic nature of online child sexual exploitation. A multi-strategy of robust legal enforcement, innovative technology, education on cyber safety, institutional capacity building, support services to victims, and cooperation between governments, technological businesses, academic institutions, civil society organisations and international agencies are essential towards effective child

protection.

It ends by concluding that cybercrime needs the involvement of children in order to protect them in cyberspace by adopting a child-centred and multidisciplinary framework of governance that involves law, technology, public policy and education to guarantee the safety, dignity, privacy and general well-being of children in the digital age.

Keywords: Online Child Sexual Exploitation, Child Sexual Abuse Material (CSAM), Cyber Law, Child Protection, Digital Safety.

1. Introduction

The high rate of digitization has changed the life of children by availing more achievements in terms of education, interactions, entertainment, and socialization. Smart phones, social media, internet based gaming and instant messaging applications has become part and parcel of the kids daily life which gives them an opportunity to get in touch, learn and get involved in the world of the web. As much as these technological advances have many educational and social advantages, they have also subjected children to new nature of cyber enabled abuse and exploitation. Out of these new menaces “Online Child Sexual Exploitation (OCSE) has turned out to be the biggest menace facing the legal systems, policymakers, technology companies and child protection agencies in the whole world.¹

Online Child Sexual Exploitation means the exploitation, harassment or manipulation of children via digital methods and online methods to exploit them sexually. It involves online grooming, Child Sexual Abuse Material (CSAM), sextortion, live-streamed sexual abuse, cyber-enabled trafficking, and social media-, online gaming-, and encrypted communication-enabled exploitation. These offenders often ignore geographical boundaries and therefore children often victims of such offenders can be located in a variety of different jurisdictions including other countries, unlike traditional types of child sexual abuse, as they enable their offenders to hide their identity and shuffle victims across different jurisdictions. The anonymity, speed and worldwide accessibility of the internet has complicated the investigations and prosecution of such crimes.²

The last decade in India has seen an unprecedented rise in internet penetration and smartphone

¹ Aparna Bhat, *Child and the Law* (2nd edn., LexisNexis, 2019).

² Jyoti Belur & Brijesh Bahadur Singh, "Child Sexual Abuse and the Law in India: A Commentary", 4 *Crime Science* 26 (2015).

usage, which has led to the increased digital engagement of the children. Online learning, online entertainment and networking have become a necessity in childhood. Nonetheless, this augmented digital exposure has resulted in augmented children susceptibility to cyber predators who abuse anonymity, fabricated identities, encrypted chat as well as advanced technologies to abuse minors. The advent of artificial intelligence (AI), deepfake tools, and cryptocurrency, have added to the list of difficulties in identifying and investigating the issue of online child sexual exploitation.³

The realisation of the severity of these menaces has made India put a legal framework to protect children in the digital world. Article 14, 15(3), 21, 39(e), and 39(f) of the Constitution guarantee that children are not exploited, and guaranteed equality and dignity. Various laws, including the Protection of Children from Sexual Offences Act, 2012 (POCSO Act), the Information Technology Act, 2000, the Bharat bara tika Sanhita, 2023, the Bharat Nagarik Sanhita, 2023, the digital personal data protection act, 2023, and the juvenile justice (care and protection of children) act, 2015, complement these constitutional protections. Another international tool used in India to fight child exploitation in cyberspace is the United Nations Convention on the Rights of the Child (UNCRC) and other international programs of fighting cybercrimes.⁴

In spite of these legislative protection, there are still major challenges. The rate of technological innovation usually surpasses legal changes, encrypted communication, transnational cyber crime, under-reporting of crimes, poor digital literacy, and poor coordination of law enforcement bodies and technological companies keep playing against meaningful enforcement. These predicaments show that online child sexual exploitation is multidimensional and thus requires legal solutions to deal with it.

It is in this context that this paper will take an interdisciplinary approach of socio-legal analysis, comprising of opinions and outlooks of law, cybersecurity, criminology, psychology, information technology and public policy. It explores the legal context of OCSE in India, the technological and institutional obstacles involved in fighting such crimes, policy measures taken and the recommendations that can be made to enhance child protection in cyberspace.

³ National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2024); Internet and Mobile Association of India & Kantar, *Internet in India Report 2023*.

⁴ Constitution of India, arts. 14, 15(3), 21, 39(e) & 39(f); Protection of Children from Sexual Offences Act, 2012; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Digital Personal Data Protection Act, 2023; Juvenile Justice (Care and Protection of Children) Act, 2015; United Nations Convention on the Rights of the Child, 1989.

The research will inform the creation of an all-embrasive, child-focused framework that will guarantee the safety, dignity, privacy and well-being of children in the fast-changing digital world.⁵

2. Understanding Online Child Sexual Exploitation

2.1 Meaning of OCSE

Online Child Sexual Exploitation (OCSE) is the exploitation, abuse or threat of children by means of digital platforms, internet services, and electronic communication technologies. These activities are online grooming, creation and distribution of Child Sexual Abuse Material (CSAM), sextortion, live-streamed sexual abuse, and other offences that are aided by technology. OCSE infringes on the basic human rights of children (the right to dignity, privacy, safety, and protection) and in many cases results in the long-term psychological and emotional damage.⁶

2.2 Online Grooming

Online grooming is an activity wherein offenders build emotional boundaries with children via social media, online games, chat rooms, or messaging applications with the view of sexual exploitation. Offenders often make up false identities, impersonate children or friends and even family members and earn the trust of the victim by manipulating them and providing emotional intimacy. As soon as confidence is gained, they might induce or threaten children to send out intimate photos, conduct dirty chats, or even meet.⁷

2.3 Child Sexual Abuse Material (CSAM)

Child Sexual Abuse Material (CSAM) is defined as a photograph, a video, audio tapes or images created digitally which portray the sexual exploitation or abuse of children. Instead of using the term child pornography, the term CSAM is a better term since it is used to associate the abusive content. The use of modern technologies allows distributing such material quickly and encrypted with the help of messaging applications, cloud storage, peer-to-peer networks,

⁵ National Crime Records Bureau, *Crime in India 2023*.

⁶ Ministry of Home Affairs, *Cyber Crime Prevention against Women and Children (CCPWC) Scheme* (Government of India).

⁷ Aparna Bhat, *Child and the Law* (2nd edn., LexisNexis, 2019).

and the dark web, which makes it even more challenging to detect, eliminate, and prosecute.

2.4 Sextortion

Sextortion is a type of Internet exploitation where sex perpetrators threaten or blackmail children with both intimate photos or videos to earn them money, additional pornographic material, or sexual favors. Fear, shame, or intimidation are used to control victims, and this greatly affects their personality resulting to severe psychological implications, like anxiety, depression, social isolation and loss of self-confidence. The transferable character of digital content can often lead to repeated victimization.⁸

2.5 Live-Streamed Child Sexual Abuse

Live-streamed child sexual abuse is the use of video conferencing or online streaming to broadcast sexual exploitation, in real-time. Abuse can be perpetrated in one place by offenders directing or funding it to be done in a different place, and thereby exploiting the jurisdictions. These crimes pose a grave problem to law enforcement agencies as a result of the cross-border aspect of the offences.⁹

2.6 Emerging Technological Challenges

The rapid technological advancements have brought with them new shapes of the connection of child sexual exploitation online. The manipulated explicit pictures can be obtained with the use of artificial intelligence and deepfake technology, encrypted systems of communication, anonymity in payment services, cryptocurrencies and the dark web allow offenders to hide the identity and stay unnoticed. Such new technology has ensured that cyber investigations are increasingly complex and demand specialist digital forensic skills.¹⁰

2.7 Impact on Children

Children who are sexually exploited by means of the Internet have severe and enduring effects. The children tend to develop a psychological trauma, anxiety, depression, post-traumatic stress disorder (PTSD), fear, loss of self-esteem and inability to form healthy relationships. Because

⁸ National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2024).

⁹ United Nations Office on Drugs and Crime, *Global Study on Sexual Exploitation of Children in the Digital Environment* (2022).

¹⁰ Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C), *Annual Report* (latest edition).

of the indefinite possibility of copying and sharing of digital material, victims will continue to be used and abused even after the first abuse. The implications of these effects emphasize the role of good legal safeguards, psychological intercessions, and preventive strategies to guarantee the safety of children in the virtual world.¹¹

3. Legal Framework Governing Online Child Sexual Exploitation

India has created a legal system to counteract Online Child Sexual Exploitation (OCSE) using constitutional, special laws, cyber laws and international undertakings. The laws are meant to defend it against sexual abuse, exploitation and invasion of privacy of children in the virtual world.¹²

3.1 Constitutional Protection

The Constitution of India forms the basis of safeguarding children against any kind of exploitation. Article 14 ensures equal protection before the law whereas Article 15(3) will grant the State the power to make special provision on women and children. Article 21 safeguards the right to life and personal liberty that extends to the right to dignity, privacy, and protection against abuse. Moreover, the Articles 39(e) and 39(f) guide the State on preserving the children against exploitation and enjoy healthy development in the circumstances of liberty and honor. Indian child protection laws are based on these constitutional protections.¹³

3.2 Protection of Children from Sexual Offences Act, 2012

The main legislation on sexual offences against children is the Protection of Children from Sexual Offences (POCSO) Act, 2012. It criminalises a broad spectrum of sexual offences such as sexual assault, sexual harassment as well as using children as pornographic material and defines a child as anyone under the age of eighteen years. The Act offers a child friendly process of reporting offences, taking evidence and investigating, and sets Special Courts to allow prompt trials of cases. It can also be used in a number of technology-mediated sexual exploitation including online grooming and the production and dissemination of sexually explicit content of children.¹⁴

¹¹ Aparna Bhat, *Child and the Law* (2nd edn., LexisNexis, 2019).

¹² *Ibid.*

¹³ M.P. Jain, *Indian Constitutional Law* (9th edn., LexisNexis, 2023).

¹⁴ Protection of Children from Sexual Offences Act, 2012, ss. 2(d), 3–15, 19–37.

3.3 Information Technology Act, 2000

Information Technology act 2000 deals with cyber-enabled offences against children. Both these sections specifically make it a criminal act to publish, transmit, browse, download or possess Child Sexual Abuse Material (CSAM) in electronic form. Other benefits of the Act include a legal basis to electronic records, which enables investigation procedures in cyber-based investigations to collect and preserve existing cyber evidence, vital in the pursuit of prosecution against child sexual offenses handled electronically.¹⁵

3.4 Bharatiya Nyaya Sanhita, 2023

Complementing the POCSO Act in 2023, the Bharatiya Nyaya Sanhita (BNS) enhances criminal law areas concerning trafficking, organised crime, extortion, criminal intimidation, and other offences committed via electronic communication. It re-forms the criminal justice system in India and allows the law enforcement to respond to the crimes against children facilitated by technologies more efficiently.¹⁶

3.5 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 also enhances privacy of children in the digital world. It needs consent of the parent to process children personal data, and limits behavioural surveillance and targeted advertisements to children. The Act curbs the chances of online grooming, identity abuse, and exploitation of children by lowering the exposure of the children to personal information online.¹⁷

3.6 International Legal Framework

Child sexual exploitation On-line child sexual exploitation is a transnational crime which needs international collaboration. India has signed the United Nations Convention on the Rights of the Child (UNCRC), 1989, which states that States should safeguard children against every kind of sexual exploitation and abuse. The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography continues to enhance international responsibility of criminalisation of child sexual abuse material. The international cooperation is enabled by

¹⁵ Information Technology Act, 2000, s. 67B.

¹⁶ K.D. Gaur, *Textbook on the Bharatiya Nyaya Sanhita, 2023* (Universal LexisNexis, latest ed.).

¹⁷ Digital Personal Data Protection Act, 2023, ss. 9 & 10.

organisations like the INTERPOL, UNICEF, and the international Telecommunication Union (ITU) through exchange of information, victim identification, capacity building and investigations of cybercrime.¹⁸

3.7 Critical Analysis

The legal system of India offers a great protection against Online Child Sexual Exploitation due to the constitutional protection, special legislation, cyber laws and international obligations. The issue of enforcement however remains a problem with encrypted communication and artificial intelligence, fake online identities, cross-national cybercrime, lack of digital forensic capacity, and insufficient technical skills. As such, the key to enhancing child protection in the digital realm is targeted legislative changes, specialised cybercrime education, increased international collaboration, and enhanced responsibility of digital platforms.¹⁹

4. Technological Dimensions of Online Child Sexual Exploitation

The high pace of digital technology development has greatly transformed the nature itself of Online Child Sexual Exploitation (OCSE) as well as the means and methods of fighting with it. Although the digital innovation has enhanced communication and access to information it has also given the offenders advanced equipment to use to exploit children. The internet allows the perpetration of these offences with anonymity, pace and accessibility all over the globe making it even harder to identify and track.²⁰

4.1 Social Media Platforms

Online grooming is increasingly being done through social media (Instagram, Facebook, Snapchat and Tik Tok). Psychopaths use email addresses to create new personae, befriend and play with emotions of children and manipulate them to provide personal details or send sexually explicit photos. The proliferation of photos and information about the place further

¹⁸ United Nations Convention on the Rights of the Child, 1989, arts. 19 & 34; Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2000; UNICEF, *Child Online Protection*; INTERPOL, *Crimes Against Children Programme*; International Telecommunication Union, *Child Online Protection Guidelines*.

¹⁹ Jyoti Belur & Brijesh Bahadur Singh, "Child Sexual Abuse and the Law in India: A Commentary", 4 *Crime Science* 26 (2015).

²⁰ Pavan Duggal, *Textbook on Cyber Law* (Universal Law Publishing, latest ed.)

predisposes children.

4.2 Online Gaming Platforms

Online games with multiple players allow participants to interact with each other in voice communication, using text, and engaging in a personal chat. Offenders abuse this technology and build up their relationships with children over some time before coming up with inappropriate dialogues or exploitative behaviour. The risks are underestimated as gamers platforms are typically considered as entertainment zones.²¹

4.3 Encrypted Communication

The privacy of users is secured by end-to-end encrypted apps like WhatsApp, Signal, and Telegram that are, on the other hand, abused by criminals to share Child Sexual Abuse Material (CSAM) and anonymously communicate. Encryption complicates the access to digital evidence by the law enforcement agencies without violating privacy rights and safeguarding the protection of children.²²

4.4 Artificial Intelligence and Deepfakes

Artificial Intelligence (AI), has a dual contribution both in fighting and enabling cybercrime. AI is also helpful in assisting investigators in detecting CSAM, indicating possible suspicious online behaviour as well as analysing digital evidence. But, deepfake technology is capable of creating sexually explicit content (warsher images or videos) of children that may seem realistic, creating new lines of exploitation and complicating investigations.²³

4.5 Dark Web and Cloud Storage

The dark web allows offenders to sell and distribute CSAM anonymously, as well as engage in transacting illegal activities with the use of cryptocurrencies. In the same way, fast storage and sharing of illegal material through cloud storage services and file sharing tools can lead to serious problems for law enforcement bodies as the illegal contents can be stored and shared

²¹ Ministry of Electronics and Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

²² Pavan Duggal, *Textbook on Cyber Law* (Universal Law Publishing, latest ed.).

²³ Ministry of Electronics and Information Technology, *Advisory on Deepfake and AI-Generated Content*; UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

in more than one jurisdiction.

4.6 Digital Forensics and Platform Accountability

Digital forensics is now a necessity of retrieving deleted files, pursuing offenders, handling metadata, and conserving digital evidence. Meanwhile, online kid safety should be improved with age verification, AI-related content control, reporting options, and collaboration with police organizations to increase safety on the online front.

4.7 Critical Analysis

The cybercrime and cybercrime detection have been enhanced by the technological innovation. Despite the use of artificial intelligence and digital forensics, as well as automated moderation tools in the process of investigation, criminals constantly use new technologies. As such, technological measures have to be accompanied with good laws, international collaboration, digital literacy, and conscientious management of platforms.²⁴

5. Policy and Institutional Responses

Winning the War on Online Child Sexual Exploitation involves governments, law enforcement agencies, schools/colleges, tech companies, civil society organisations, and international organisations working to counter this unacceptable practice. India has embraced multiple policy measures to enhance child protection over the digital realm.

5.1 National Cyber Crime Reporting Portal

The National Cyber Crime Reporting Portal allows victims or their designated guardians to report in cyber offences, such as internet-related child sexual exploitation, cyber grooming, and distribution of Child Sexual Abuse Material (CSAM). It helps swift investigation and helps to eliminate illegal content in digital sources.

5.2 Indian Cyber Crime Coordination Centre (I4C)

Indian Cyber Crime Coordination Centre (I4C) is the nodal body of coordinating the investigation of cybercrimes, building powers to support digital forensics, capacity building

²⁴ Jyoti Belur & Brijesh Bahadur Singh, "Child Sexual Abuse and the Law in India: A Commentary", 4 *Crime Science* 26 (2015).

programmes, as well as creating cyber awareness to law enforcement organizations and common citizens.²⁵

5.3 National Commission for Protection of Child Rights (NCPCR)

The National Commission Protection of Child Rights (NCPCR) oversees the laws that are implemented to protect children, conducts awareness campaigns, grievance concerns on children rights, and enhances child-friendly policies and rehabilitation efforts.

5.4 Role of Educational Institutions

The schools have a significant preventative role through the provision of digital literacy and cyber safety courses. Children need to be taught by teachers and counsellors the basics of grooming on the internet, cyberbullying, protection of internet privacy and safe internet practices and learn how to detect indications of abuse by an online community.

5.5 Role of Parents and Technology Companies

Parents ought to be keen on supervising the online activities of children, promote responsible internet usage as well as settings up communication on the risks involved online should be maintained. In order to enhance child safety, technology companies are encouraged to enhance their age verification, content moderation, reporting, privacy, and collaboration with law enforcement agencies.²⁶

5.6 International Cooperation

Because Online Child Sexual Exploitation often involves offenders acting internationally, cross-border cooperation in the form of international information sharing, legal assistance with each other, sharing computer evidence, and cross-country cybercrime investigations is a required part of successful investigation. Organisations like UNICEF and INTERPOL are key in supporting the international cooperation.

²⁵ Ministry of Home Affairs, *Indian Cyber Crime Coordination Centre (I4C): Annual Report* (latest ed.).

²⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, Government of India.

5.7 Critical Analysis

India has put in place a number of institutional mechanisms which deal with Online Child Sexual Exploitation. Nevertheless, the issue of ineffective digital infrastructure, a lack of trained cyber investigators, under-reporting of crimes, lack of awareness among the population, and poor coordination among agencies still impede successful implementation. Enhancing both institutional capacity and relations between the public and the private sphere, as well as reinforce private cooperation and collaboration at an international level are crucial to effective child protection in cyberspace.²⁷

6. Recommendations

The multi-disciplinary strategy is necessary to effectively deal with Online Child sexual Exploitation (OCSE) issue. Making the cyberspace safer to child protection can be enhanced by the following recommendations:

1. Enforce the Legal Framework: The existing cyber laws need to be reviewed and revised on a regular basis to accommodate new technologies like Artificial Intelligence (AI)-generated Child Sexual Abuse Material (CSAM), deepfakes, virtual reality services and virtual communication services that would be encrypted. Well defined legal provisions and harsher punishments will enhance enforcement and make the law marketable in line with the technological advancement.

2. Strengthen Cyber Investigation Capacity: The governments are to create specialised cybercrime departments with state-of-the-art digital forensic-testing laboratories and up-to-date investigative equipment. The police officers, prosecutors, judges and forensic experts should give regular training to enhance the ability of the police to investigate and prosecute technology enabled offences.

3. Uplift Responsibility in Platforms: Social media, online games, messaging platforms, and internet services providers must ensure there are more effective age verification systems, AI-enhanced regulation of content, effective reporting policies, and timely elimination of illicit materials. More coordination with law enforcement agencies also needs to be done.

²⁷ Pavan Duggal, *Textbook on Cyber Law* (Universal Law Publishing, latest ed.).

4. Advance Digital Awareness and literacy: This should be made mandatory through school programs that will teach children the ways of grooming their selves online, protect their privacy, cyberbullying, sextortion and safe internet usage. Parents, teachers, and communities should also be used in the awareness programmes to enhance online safety.

5. Enhance Victim Support Services: Child victims are supposed to be provided with counselling, legal support, medical treatment, rehabilitation and child friendly reporting systems. Psychological support and reintegrating a victim into the community as soon as possible are crucial in minimising the effects of a victim on their long-term life.

6. Enhance Institutional Co-ordination: There is a need to use effective coordination among law enforcement agencies, children protection authorities, schools and colleges and both technical and non-technical societies to control online child sexual exploitation and rehabilitate victims.

7. Increase International Collaboration: Online child sexual exploitation oftentimes involves cross-border crimes, and nations need to enhance both information sharing, mutual legal support, digital evidence sharing, as well as collaborations in cyber criminal investigations via international organisations and bilateral partnerships.

7. Conclusion

The high growth rate of digital technology has changed the life of children because it brings in new possibilities in the areas of learning, communicating and socializing. It has however also gotten them more exposed to growing threats of increasing risks of Online Child Sexual Exploitation (OCSE) such as online grooming, Child Sexual Abuse Material (CSAM), sextortion and live-streamed sexual abuse. These offences have increasingly become complex and challenging to probe due to the increased use of artificial intelligence, coded messages, unidentity platforms, and the emergence of new technologies on the internet. India has established an elaborate legal system via the Constitution of India, Protection of Children of Sexual Offences Act, 2012, Information Technology Act, 2000, the Bharotiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023. These laws give a high level of legal safeguards to children but, due to the influence of technology, inter-country internet crimes, the lack of digital forensics capacity, under-reporting, and poor inter-agency liaisons, there are still challenges to its effective implementation. This paper illustrates that online child sexual

exploitation is too complicated and dynamic to be dealt with solely by legal control. Multiple disciplines of law, technology, cybersecurity, education, psychology, and public policy” are necessary to build a framework of more effective child protection. Strengthened cyber investigation, digital literacy, platform responsibility, support services to victims and international collaboration are other essential aspects that will make the digital world safer. The governments, law enforcers, technology companies, institutions of learning, and parents together with civil societies organisations and international community all have a role to play in ensuring the children are safe in cyberspace. Such a technology- responsive and child-based governance framework will not only enhance the prevention and prosecution of crime against children on the internet but also make the digital world safe, secure and dignified so that every child can access and benefit.