

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Online Child Sexual Abuse and Exploitation (OCSAE): Emerging Challenges Before India's Juvenile Justice Framework in the Digital Age

SUMIT KUMAR*  AND DR. BIMALDEEP SINGH**

ABSTRACT

Over the last few years children's use of the internet has increased rapidly. Online classes after the COVID-19 pandemic, affordable smartphones and easy access to social media have made digital platforms a regular part of everyday life. Children now use the internet to attend classes, talk to friends, watch videos, play games and search for information. Digital technology has made many everyday activities easier, but it has also exposed children to risks that were far less common a few years ago. Among these risks, Online Child Sexual Abuse and Exploitation (OCSAE) has become a major concern. Offenders use a range of online platforms to contact children and gradually gain their trust. In many cases children are threatened through sextortion, or their abusive images and videos are circulated without their consent. The misuse of artificial intelligence has made the situation more worrying still, because deepfake technology and other AI tools can now create fake but realistic abusive images and videos within a very short time, which makes detection and investigation more difficult. India has enacted a number of laws to protect children, and these laws provide the legal basis for dealing with offences committed against them. Most of them, however, were enacted before the present pace of technological change. As technology continues to change, investigating agencies face new problems such as encrypted messaging, fake online identities, foreign servers, cross-border cyber offences and AI-generated abuse material, and these developments have made investigation, prosecution and victim protection considerably harder than before. They also show that the existing legal system must continue to evolve if it is to address new forms of online child exploitation. This study examines the nature and different forms of OCSAE and analyses whether India's juvenile justice framework is capable of dealing with these emerging digital offences. It also discusses the forms of online child sexual abuse and exploitation, their causes and the relevant international legal instruments.

* Author is a Research Scholar at Department of Laws, Guru Nanak Dev University, Amritsar, Punjab, India. ORCID: <https://orcid.org/0009-0001-6804-2579>

** Author is an Associate Professor at Department of Laws, Guru Nanak Dev University, Amritsar, Punjab, India.

Keywords: *Online Child Sexual Abuse and Exploitation (OCSAE), Child Sexual Exploitation and Abuse Material (CSEAM), juvenile justice, POCSO, artificial intelligence, cybercrime, digital evidence, child rights, online grooming*

I. INTRODUCTION

The twenty-first century has witnessed an unprecedented growth in digital technology. The internet has become an essential part of everyday life and has changed the way people communicate, learn, work and access information. Children are among the largest users of digital technologies. They use smartphones, tablets, laptops and the internet for education, entertainment, social networking and online gaming. Digital platforms have created new opportunities for learning and personal development, but they have also exposed children to risks that were either unknown or very limited in the past. One of the most serious concerns emerging from this transformation is the increasing incidence of Online Child Sexual Abuse and Exploitation (OCSAE).¹

India has experienced rapid digital growth over the last decade. Affordable smartphones, cheaper internet services and government initiatives promoting digital connectivity have significantly increased internet access across the country. The COVID-19 pandemic accelerated that process further. During the nationwide lockdown, schools, colleges and coaching institutions shifted to online classes, and children consequently spent considerably more time on digital devices for educational as well as recreational purposes. Online education helped the learning process to continue, but it also increased children's exposure to cyber risks, because many children accessed the internet without adequate parental supervision or sufficient awareness of online safety.²

The digital environment has created new methods through which offenders can target children. Unlike conventional forms of child sexual abuse, many online offences take place without any physical contact between the offender and the victim. Offenders create fake social media profiles, join online gaming platforms or use messaging applications to establish contact with children, and gradually gain a child's trust by pretending to be a friend or someone of a

¹ UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Online Child Sexual Exploitation and Abuse*, in E4J UNIVERSITY MODULE SERIES: CYBERCRIME, Module 12 (Interpersonal Cybercrime), available at <https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html> (last visited June 26, 2026).

² INTERNET AND MOBILE ASSOCIATION OF INDIA & KANTAR, *Internet in India Report 2023* (IAMAI, released February 27, 2024, based on the ICUBE 2023 study) (recording 820 million active internet users and internet penetration above 55 per cent); COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, U.N. Doc. CRC/C/GC/25 (March 2, 2021), paras. 84-86.

similar age. This process, commonly known as online grooming, is usually the first step towards sexual exploitation.³

Another form of online exploitation is sextortion. In such cases offenders obtain intimate images or videos of children and later use them to blackmail or threaten the victim. The child may be forced to send additional sexual content, to perform sexual acts during video calls or even to pay money to prevent the material from being shared publicly. Fear of social stigma, family reactions and public humiliation often prevents victims from reporting these offences, which allows offenders to continue their criminal activities.⁴

The internet has also made it easier to produce, store and circulate Child Sexual Exploitation and Abuse Material (CSEAM). Such content was earlier described as “child pornography”. International organisations and recent judicial developments have recognised, however, that this expression fails to reflect the seriousness of the offence because it may suggest consent or voluntary participation. The term Child Sexual Exploitation and Abuse Material is now preferred because it recognises that every such image or video represents the sexual abuse and exploitation of a child, and because it places the focus on the child as a victim rather than on the material itself.⁵

Recent technological developments have complicated the problem further. Artificial intelligence now enables the creation of highly realistic fake images and videos through deepfake technology. Such digitally generated images may depict children in sexually explicit situations even where no actual abuse has taken place.⁶

Another major challenge is the increasing use of encrypted messaging applications and the dark web. End-to-end encryption protects ordinary users from hacking and from unauthorised access to their private conversations, but the same technology can also be misused by offenders to exchange abusive material without ready detection by investigating agencies. The dark web, similarly, provides anonymous platforms on which Child Sexual Exploitation and Abuse Material may be bought, sold or shared among organised criminal networks operating across different countries. These developments make investigation, evidence collection and prosecution considerably more difficult than in ordinary criminal cases.⁷

³ COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2, paras. 80-81.

⁴ WEPROTECT GLOBAL ALLIANCE, *Global Threat Assessment 2023: Assessing the Scale and Scope of Child Sexual Exploitation and Abuse Online* (WeProtect Global Alliance, 2023).

⁵ *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716, Criminal Appeal Nos. 2161-2162 of 2024, decided on September 23, 2024.

⁶ EUROPOL INNOVATION LAB, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (Publications Office of the European Union, Luxembourg, 2022).

⁷ UNODC, *supra* note 1.

A. Rise of OCSAE

The growing use of digital technologies has therefore changed the nature of crimes against children. OCSAE is no longer merely a cybercrime or an issue of information technology. It has become a serious child protection and human rights concern, because it affects a child's physical safety, mental health, privacy, dignity and overall development. The consequences of online abuse often continue even after the offence has ended, since digital content can be copied, stored and circulated repeatedly. Child victims may therefore experience continuing trauma and fear long after the original abuse has occurred.⁸

India has enacted several important laws to safeguard children. The Constitution of India, the Juvenile Justice (Care and Protection of Children) Act, 2015, the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000 together provide an important legal framework for protecting children from abuse and exploitation. Rapid technological change, artificial intelligence, encrypted communication, cross-border cybercrime and emerging forms of digital exploitation have nonetheless exposed several limitations within that framework.

B. Statement of the problem

India has enacted several laws to protect children from abuse, neglect and exploitation. The Constitution of India guarantees various rights to children, while the Juvenile Justice (Care and Protection of Children) Act, 2015, the Protection of Children from Sexual Offences Act, 2012 (POCSO) and the Information Technology Act, 2000 provide legal safeguards against different forms of child abuse, including offences committed through digital platforms. These laws have strengthened child protection in many respects. The rapid growth of digital technology has, however, created new forms of online child sexual abuse and exploitation that were not fully anticipated when most of these laws were enacted.⁹

Online Child Sexual Abuse and Exploitation has become more organised and technologically advanced. Offenders now use social media platforms, encrypted messaging services, online gaming applications, artificial intelligence, deepfake technology and anonymous online networks to target children. These developments have made the detection, investigation and prosecution of offenders much more difficult. Since many offences are committed across

⁸ COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2.

⁹ The Juvenile Justice (Care and Protection of Children) Act, 2015 (Act 2 of 2016); The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012); The Information Technology Act, 2000 (Act 21 of 2000).

national borders, law enforcement agencies also face jurisdictional and procedural difficulties while collecting digital evidence and identifying offenders.¹⁰

Although India has enacted separate laws dealing with child protection and with cyber offences, there is no single legislative framework addressed specifically to Online Child Sexual Abuse and Exploitation.

Existing laws are directed mainly at the investigation and punishment of offenders, while comparatively less attention has been given to long-term counselling, psychological support, digital privacy and the rehabilitation of child victims. These issues require greater attention within India's juvenile justice framework.¹¹

In view of these challenges, it becomes necessary to examine whether the existing juvenile justice system is capable of responding effectively to technology-driven offences against children. This study analyses the legal and institutional gaps in the present framework and suggests reforms capable of strengthening the protection of children in the digital environment.

C. Research questions

The present study seeks to answer the following research questions.

What constitutes Online Child Sexual Abuse and Exploitation, and what are its different forms in the digital environment?

Is the existing juvenile justice framework in India adequately equipped to prevent, investigate and respond to Online Child Sexual Abuse and Exploitation?

What are the major legal, technological and institutional challenges faced by law enforcement agencies and by the juvenile justice system in investigating and prosecuting OCSAE-related offences?

D. Research objectives

The present study has been undertaken with the following objectives.

To study the concept, meaning and different forms of Online Child Sexual Abuse and Exploitation in the digital environment.

To examine the international legal standards and child rights instruments relating to the prevention of online child sexual abuse and exploitation.

¹⁰ UNODC, *supra* note 1.

¹¹ UNICEF, *The State of the World's Children 2021: On My Mind - Promoting, Protecting and Caring for Children's Mental Health* (UNICEF, New York, October 2021); WEPROTECT GLOBAL ALLIANCE, *Global Strategic Response to End Child Sexual Exploitation and Abuse Online* (WeProtect Global Alliance, 2021).

To identify the legal, technological and institutional challenges faced by the juvenile justice system in investigating, prosecuting and preventing offences relating to Online Child Sexual Abuse and Exploitation.

To suggest legal and policy reforms capable of strengthening India's juvenile justice framework so as to provide better protection to children against emerging forms of online sexual abuse and exploitation.

II. UNDERSTANDING ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION

A. Meaning and concept

Online Child Sexual Abuse and Exploitation refers to any act in which digital technology or the internet is used to sexually abuse, exploit or harm a child. Such offences may take place through social media platforms, online games, messaging applications, websites, video-sharing platforms or other digital services. The abuse may involve direct communication with a child, the sharing of sexually explicit material, the live-streaming of abuse, online grooming, or the creation and distribution of abusive images and videos. Unlike traditional offences, OCSAE can be committed without physical contact between the offender and the child, which makes detection and investigation more difficult.¹²

Several expressions are used in discussions of child sexual abuse on the internet. Although these terms are related, they do not carry the same meaning.

The expression child sexual abuse refers to any sexual act committed against a child. It includes both physical and non-physical forms of abuse. A child may be forced, threatened, deceived or manipulated into participating in sexual activity. Such abuse may occur within the family, in educational institutions, in the neighbourhood or through online platforms. Child sexual abuse is therefore a broad concept covering all forms of sexual violence against children.¹³

Child sexual exploitation is a wider concept than child sexual abuse. It occurs where a child is sexually abused for the benefit, profit or advantage of another person, and that benefit may be financial, social or personal. Exploitation includes activities such as online grooming, trafficking, forced prostitution, the live-streaming of sexual abuse and the production or distribution of abusive material. Every case of child sexual exploitation therefore involves abuse, although not every case of child sexual abuse amounts to exploitation.¹⁴

¹² UNODC, *supra* note 1.

¹³ COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 13 (2011): The Right of the Child to Freedom from All Forms of Violence*, U.N. Doc. CRC/C/GC/13 (April 18, 2011), para. 25.

¹⁴ INTERAGENCY WORKING GROUP ON SEXUAL EXPLOITATION OF CHILDREN, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (adopted at Luxembourg, January 28, 2016;

The term child sexual abuse material describes photographs, videos or any visual material that records the actual sexual abuse of a child. The expression recognises that such images are evidence of a criminal offence and not ordinary pornographic material. Many international organisations have replaced the term “child pornography” with child sexual abuse material, because the earlier expression fails to reflect the fact that children can neither legally nor voluntarily consent to such acts.¹⁵

In recent years the expression Child Sexual Exploitation and Abuse Material has gained wider acceptance. It is broader than child sexual abuse material because it covers material depicting both the sexual abuse and the sexual exploitation of children. It acknowledges that every such image or video is a record of abuse and exploitation and that the child shown in the material is always a victim. The terminology also reflects a child-centred approach, since it recognises the dignity and the rights of the child instead of focusing only on the sexual content.¹⁶

The term “child pornography” was formerly used in legislation, in judicial decisions and in public discourse. That expression has now been strongly criticised by child rights organisations, international bodies and legal scholars. The word “pornography” ordinarily refers to material produced with the consent of adults for sexual purposes, and using the same expression for material involving children is misleading, because a child can never lawfully consent to sexual exploitation. The term may also reduce the apparent seriousness of the offence by treating abusive material as a category of pornography instead of recognising it as evidence of child abuse. For these reasons international bodies, including the United Nations Office on Drugs and Crime, UNICEF and the WeProtect Global Alliance, recommend the use of “Child Sexual Exploitation and Abuse Material” or “child sexual abuse material”.¹⁷

The Supreme Court of India has likewise recognised the importance of appropriate terminology. In *Just Rights for Children Alliance v. S. Harish*, the Court observed that the expression “child pornography” does not accurately describe the nature of the offence, because it ignores the abuse suffered by the child.¹⁸ The Court put the courts on notice that the term “child pornography” shall not be used in any judicial order or judgment and that the term “child sexual exploitation and abuse material” should be endorsed instead. Separately, and by way of

ECPAT International, Bangkok, 2016) (the Luxembourg Guidelines).

¹⁵ UNODC, *supra* note 1.

¹⁶ WEPROTECT GLOBAL ALLIANCE, *Global Strategic Response to End Child Sexual Exploitation and Abuse Online*, *supra* note 11; INTERAGENCY WORKING GROUP ON SEXUAL EXPLOITATION OF CHILDREN, *Terminology Guidelines*, *supra* note 14.

¹⁷ INTERAGENCY WORKING GROUP ON SEXUAL EXPLOITATION OF CHILDREN, *Terminology Guidelines*, *supra* note 14; UNODC, *supra* note 1.

¹⁸ *Just Rights for Children Alliance v. S. Harish*, *supra* note 5, paras. 226-228.

suggestion rather than direction, it recommended that Parliament should seriously consider amending the POCSO Act to the same effect. According to the Court, adopting this terminology shifts the focus from the material itself to the exploitation of the child and reinforces a victim-centred approach consistent with constitutional values and international child rights standards.¹⁹

B. Forms of online child sexual abuse and exploitation

Online Child Sexual Abuse and Exploitation is not confined to any single offence. With the rapid development of digital technology, offenders have adopted different methods of targeting children through the internet. These offences are often interconnected, and a child may become the victim of more than one form of online exploitation. Some of the common forms of OCSAE are discussed below.

i. Online grooming

Online grooming is one of the most common forms of online child sexual exploitation. It is a process through which an offender gradually gains the trust of a child by communicating through social media, online games, chat applications or other digital platforms. The offender often pretends to be a child of a similar age or someone who genuinely cares for the victim. Once trust has been established, the offender may persuade the child to share personal information, intimate photographs or videos, and in some cases the child is manipulated into meeting the offender in person for sexual purposes. Because grooming usually develops over a period of time, many children fail to recognise that they are being exploited until it is too late.²⁰

ii. Sextortion

Sextortion is another serious form of online exploitation. The offender obtains intimate photographs or videos of a child and later threatens to share them publicly unless the child meets certain demands. Those demands may include sending further sexually explicit images, participating in live video calls or paying money. Fear of public embarrassment often prevents children from reporting such incidents to their parents or to the police, with the result that offenders are able to exploit the victim over a long period.²¹

iii. Live-streaming of child sexual abuse

Live-streaming refers to the real-time broadcasting of child sexual abuse over the internet. Offenders either direct the abuse through online communication or pay another person to carry it out while watching from another location. Because the abuse is transmitted instantly,

¹⁹ *Id.*, paras. 260(i)-(ii); UNODC, *supra* note 1.

²⁰ UNODC, *supra* note 1.

²¹ WEPROTECT GLOBAL ALLIANCE, *Global Threat Assessment 2023*, *supra* note 4.

offenders may avoid creating permanent recordings, which makes investigation more difficult. This form of exploitation has become a growing concern because it often involves organised criminal networks operating across different countries.²²

iv. Self-generated sexual content

Self-generated sexual content refers to intimate photographs or videos created by children themselves, either voluntarily or under pressure from another person. Many children share such material in the belief that it will remain private between friends or romantic partners. The content may later be circulated without their consent, leading to blackmail, harassment or further sexual exploitation.²³

v. AI-generated child sexual exploitation and abuse material

AI-generated Child Sexual Exploitation and Abuse Material is material depicting the sexual abuse or exploitation of a child that has been produced or altered using artificial intelligence. It may be created by combining existing photographs with artificial image-generation technology. Although such images are digitally generated, they can still cause serious harm to children by violating their dignity and privacy. The rapid growth of AI-generated CSEAM has raised important legal questions about criminal liability, detection and regulation.²⁴

vi. Deepfake child abuse

Deepfake technology uses artificial intelligence to substitute one person's face or voice for another in a photograph or video. Where a child's face is digitally inserted into sexually explicit material, the result is described as deepfake child abuse. Such content may appear genuine even though the child never participated in the act shown. The circulation of deepfake material can seriously damage a child's reputation and mental health, and it also creates difficulties for investigators, because identifying fabricated content ordinarily requires specialised digital forensic techniques.²⁵

vii. Dark web marketplaces

The dark web is a hidden part of the internet that cannot be reached through ordinary search engines. It offers users a high degree of anonymity, which makes it attractive for organised criminal activity. Some dark web marketplaces are used for the buying, selling and exchange of Child Sexual Exploitation and Abuse Material. Such platforms often operate across several

²² UNODC, *supra* note 1.

²³ COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2, para. 81.

²⁴ EUROPOL INNOVATION LAB, *supra* note 6.

²⁵ EUROPOL INNOVATION LAB, *supra* note 6.

countries and use cryptocurrencies for payment, which makes it difficult for law enforcement agencies to trace offenders and dismantle criminal networks.²⁶

viii. Encrypted messaging applications

Many messaging applications now provide end-to-end encryption in order to protect the privacy of their users. Encryption is an important feature of secure communication, but it may also be misused by offenders to exchange abusive material without ready detection. Child sexual abuse material, grooming conversations and illegal images can be shared through encrypted applications, which complicates investigation. Investigating agencies frequently face difficulties in accessing digital evidence because the service providers themselves may have no access to the content of encrypted communications.²⁷

These forms of Online Child Sexual Abuse and Exploitation show that technology has significantly changed the methods used by offenders to target children. The offences are becoming more sophisticated through the use of artificial intelligence, encrypted communication and anonymous online networks. Addressing OCSAE therefore requires not only strong criminal laws but also effective cyber investigation, international cooperation, digital awareness and child-centred protection mechanisms.

C. Causes of online child sexual abuse and exploitation

The rapid increase in Online Child Sexual Abuse and Exploitation is the result of several social, technological and legal factors. The expansion of digital technology has brought many benefits, but it has also created new opportunities for offenders to target children. Understanding the causes of OCSAE is important because it assists in developing effective laws, preventive measures and child protection policies.

i. Cheap and easy internet access

One of the principal reasons behind the rise of OCSAE is the widespread availability of affordable internet services. Mobile data tariffs in India are low, and internet access has expanded rapidly, including in rural and economically weaker areas. Children can now reach social media platforms, gaming applications and websites through smartphones with little difficulty. Digital connectivity has improved education and communication, but it has also increased children's exposure to online offenders. Easy internet access without adequate safeguards has therefore become an important contributing factor to online child exploitation.²⁸

²⁶ UNODC, *supra* note 1.

²⁷ UNODC, *supra* note 1; COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2.

²⁸ INTERNET AND MOBILE ASSOCIATION OF INDIA & KANTAR, *Internet in India Report 2023*, *supra* note 2.

ii. Increasing use of social media

Social media has become an important part of children's daily lives. Platforms that allow users to share photographs, videos and personal information have made communication easier, but heavy use of social media has also increased children's vulnerability. Many children accept friend requests from strangers, take part in online challenges or share personal details without understanding the possible consequences. Offenders monitor children's online activity, identify vulnerable users and establish contact through fake profiles. In many cases online grooming begins on a social networking platform before moving to private messaging applications.²⁹

iii. Lack of parental supervision

Many parents are unaware of their children's online activities. Busy work schedules, limited digital knowledge and the increasing use of personal devices often reduce parental supervision. During the COVID-19 pandemic children spent longer hours online for education as well as entertainment, and in many households parents encouraged digital learning but were unable to monitor how children used the internet once classes had ended. A lack of communication between parents and children about online safety further increases the possibility of exploitation. Children who receive no guidance about privacy settings, online strangers and safe internet practices are more likely to become victims of cyber offences.³⁰

iv. Anonymous online platforms

The internet allows users to create anonymous accounts without disclosing their true identity. Many social media platforms, gaming applications and discussion forums require only basic information to open an account. Offenders misuse that anonymity by creating fake identities and pretending to be children or trusted adults, which makes it easier to approach children without arousing suspicion. The ability to remain anonymous also makes it difficult for investigating agencies to identify offenders and to collect reliable digital evidence.³¹

v. Use of cryptocurrency

Organised criminal groups sometimes use cryptocurrencies to purchase, sell or distribute Child Sexual Exploitation and Abuse Material through illegal online networks. Because cryptocurrency transactions may involve users located in different countries, tracing financial

²⁹ COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2, para. 81; UNODC, *supra* note 1.

³⁰ COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2, paras. 84-86.

³¹ UNODC, *supra* note 1.

flows becomes more difficult for law enforcement agencies. This has strengthened the financial networks that support online child exploitation.³²

vi. Misuse of artificial intelligence

Artificial intelligence is among the most significant technological developments of recent years. Although it has many beneficial uses, it can also be misused to facilitate child sexual exploitation. AI-powered image generation, voice cloning and deepfake technology can produce realistic sexually explicit images or videos involving children, and such material may be used for blackmail, online harassment or further exploitation. AI tools also allow offenders to create fake identities, to automate online conversations and to target several victims at once. These developments have made the detection of online offences more complicated than before.³³

III. INTERNATIONAL LEGAL FRAMEWORK

A. United Nations Convention on the Rights of the Child

The Convention on the Rights of the Child, 1989 is the most important international treaty for the protection of children's rights. India acceded to the Convention on 11 December 1992 and is therefore under an obligation to adopt appropriate legislative, administrative and social measures to protect children from all forms of abuse and exploitation. Although the Convention was adopted before the rapid expansion of the internet and of digital technologies, its principles continue to apply to the online environment.³⁴

Several provisions of the Convention bear directly on Online Child Sexual Abuse and Exploitation. Article 19 requires States Parties to protect children from all forms of physical or mental violence, injury, abuse, neglect, maltreatment and exploitation while they are in the care of parents, guardians or any other person.³⁵ Article 34 requires States to protect children from every form of sexual exploitation and sexual abuse and to adopt effective measures to prevent such offences.³⁶ Article 35 obliges States to take all appropriate national, bilateral and multilateral measures to prevent the abduction, sale and trafficking of children for any purpose and in any form.³⁷ Article 36 further provides that children must be protected against every other

³² FINANCIAL ACTION TASK FORCE, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (FATF, Paris, September 14, 2020); UNODC, *supra* note 1.

³³ INTERNET WATCH FOUNDATION, *How AI Is Being Abused to Create Child Sexual Abuse Imagery* (IWF, October 2023).

³⁴ Convention on the Rights of the Child, adopted November 20, 1989, entered into force September 2, 1990, 1577 U.N.T.S. 3; India acceded on December 11, 1992.

³⁵ *Id.*, art. 19.

³⁶ *Id.*, art. 34.

³⁷ *Id.*, art. 35.

form of exploitation prejudicial to their welfare.³⁸ Article 39 places a duty on States to promote the physical and psychological recovery and the social reintegration of children who have suffered abuse, neglect or exploitation.³⁹

The rights guaranteed under the Convention have been explained further by the Committee on the Rights of the Child in General Comment No. 25 (2021) on children's rights in relation to the digital environment. The Committee recognised that children enjoy the same rights in the digital environment as they do offline. It called upon States to enact effective laws, to strengthen online safety measures, to regulate digital service providers, to improve digital literacy among children and parents, and to ensure accessible reporting mechanisms and child-friendly remedies for victims of online abuse. The General Comment also emphasises that the best interests of the child must remain a primary consideration in the development of laws and policies relating to digital technologies.⁴⁰

The Convention and General Comment No. 25 together establish an important international framework for protecting children against online sexual abuse and exploitation. They make it clear that child protection in the digital age is not only a national responsibility but also an international legal obligation, and they supply useful standards against which the adequacy of the Indian legal framework, and of the juvenile justice system in particular, may be examined. The following section therefore considers the international instruments that address cybercrime and online child sexual exploitation specifically, before turning to the Indian framework.

B. Optional Protocol on the sale of children, child prostitution and child pornography

The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography was adopted by the United Nations General Assembly on 25 May 2000 in order to strengthen the protection provided under the Convention. Recognising that children require special protection against sexual exploitation, the Protocol obliges States Parties to criminalise offences relating to the sale of children, child prostitution and child pornography. India signed the Protocol on 15 November 2004 and ratified it on 16 August 2005, thereby accepting the responsibility to adopt effective legislative, administrative and judicial measures to prevent these offences and to secure the protection and rehabilitation of child victims.⁴¹

³⁸ *Id.*, art. 36.

³⁹ *Id.*, art. 39.

⁴⁰ COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2, paras. 12-14, 82, 113-116.

⁴¹ Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, adopted May 25, 2000, entered into force January 18, 2002, 2171 U.N.T.S. 227; India signed on November 15, 2004 and ratified on August 16, 2005.

The Protocol defines the sale of children as any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration.⁴² Such practices may occur for several unlawful purposes, including sexual exploitation, forced labour, illegal adoption and trafficking. Although the Protocol was adopted before the rapid expansion of digital technologies, its provisions are broad enough to cover situations in which children are recruited, advertised or exploited through online platforms and digital communication.

The Protocol further requires States to prohibit child prostitution, which involves the use of a child in sexual activities in exchange for money or any other form of consideration.⁴³ In the digital environment this offence has taken new forms. Offenders increasingly use social media platforms, encrypted messaging applications, video-calling services and live-streaming technologies to exploit children, and in many cases the offender and the victim are located in different countries, which makes investigation and prosecution more difficult.

Another important feature of the Protocol is its requirement that States criminalise the production, distribution, dissemination, importation, exportation, offering, sale and possession of child pornography.⁴⁴ International organisations, child rights experts and courts have nonetheless criticised the continued use of that expression. The term may incorrectly suggest that the material is comparable to adult pornography produced with consent, whereas every image or video involving the sexual depiction of a child is evidence of abuse and exploitation. The expression Child Sexual Exploitation and Abuse Material is therefore now widely preferred, because it reflects the true nature of the offence and recognises the child as a victim rather than as an object of pornography.⁴⁵

The Supreme Court of India adopted this child-centred approach in *Just Rights for Children Alliance v. S. Harish*, where it observed that the expression “child pornography” is inaccurate and inconsistent with the dignity and rights of children. The Court directed that the term must not be used in any judicial order or judgment and that “child sexual exploitation and abuse material” should be endorsed instead, and it suggested that Parliament consider amending the POCSO Act correspondingly. Appropriate terminology matters, in the Court’s view, because it acknowledges that every such image or video is the product of sexual abuse and exploitation and not merely a form of pornographic content.⁴⁶

⁴² *Id.*, art. 2(a).

⁴³ *Id.*, art. 2(b).

⁴⁴ *Id.*, arts. 2(c) and 3(1)(c).

⁴⁵ UNODC, *supra* note 1; INTERAGENCY WORKING GROUP ON SEXUAL EXPLOITATION OF CHILDREN, *Terminology Guidelines*, *supra* note 14.

⁴⁶ *Just Rights for Children Alliance v. S. Harish*, *supra* note 5, paras. 226-228, 260(i)-(ii).

The Optional Protocol also recognises that punishment alone cannot adequately address offences involving children. It requires States Parties to ensure appropriate assistance for the physical and psychological recovery, social reintegration and rehabilitation of child victims.⁴⁷ It further provides for international cooperation through extradition, mutual legal assistance, the exchange of information and cooperation among law enforcement agencies, in recognition of the fact that offences involving online child sexual exploitation frequently extend beyond national boundaries.⁴⁸

C. Lanzarote Convention: protection against sexual exploitation and online grooming

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 2007, commonly known as the Lanzarote Convention, is one of the most comprehensive international instruments dealing exclusively with child sexual exploitation and abuse. The Convention requires States to adopt legislative, administrative and educational measures to prevent child sexual abuse, to protect child victims and to prosecute offenders. Unlike earlier international instruments, it addresses the risks posed by digital technologies expressly: Article 23 requires the criminalisation of the solicitation of children for sexual purposes through information and communication technologies, and Article 20 covers offences relating to child pornography, including knowingly obtaining access to such material through such technologies.⁴⁹

IV. EMERGING CHALLENGES BEFORE INDIA'S JUVENILE JUSTICE SYSTEM

The increasing use of digital technologies has transformed the nature of child sexual exploitation. Offences formerly involved physical contact between the offender and the child. Children today spend a large part of their time on the internet, and the same online platforms are being misused by offenders. Social media, online games, encrypted messaging applications and live-streaming services have become common means of approaching and exploiting children. The growing use of artificial intelligence has made the problem more serious still, because fake but realistic abusive images and videos can now be created within minutes.

Many of these offences are difficult to investigate. Offenders conceal their identity by using fake accounts, virtual private networks or encrypted applications. In some cases the victim is in one country, the offender in another, and the digital evidence stored on servers located

⁴⁷ Optional Protocol, *supra* note 41, art. 9(3).

⁴⁸ *Id.*, arts. 5 and 10.

⁴⁹ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, opened for signature at Lanzarote, October 25, 2007, entered into force July 1, 2010, arts. 20 and 23.

somewhere else again, which makes investigation and prosecution considerably more complicated for law enforcement agencies.

India has enacted laws such as the Juvenile Justice (Care and Protection of Children) Act, 2015, the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, which, together with the Bharatiya Nagarik Suraksha Sanhita, 2023, replaced the Indian Penal Code, 1860 and the Code of Criminal Procedure, 1973 with effect from 1 July 2024. These laws provide an important legal foundation, but many practical problems continue to affect their implementation. Investigating agencies face delays in collecting digital evidence, in tracing offenders and in coordinating with authorities in other countries. The following discussion examines these challenges and their effect on the capacity of India's juvenile justice system to deal with Online Child Sexual Abuse and Exploitation.

A. Jurisdiction

Jurisdiction is one of the most difficult issues in cases of Online Child Sexual Abuse and Exploitation. Unlike ordinary crimes, these offences do not usually occur in a single place. A child may be living in India, the offender may be operating from another country, and the abusive images or videos may be stored on a server located elsewhere. In such a situation it becomes difficult to determine which country's law applies and which authority should investigate the offence.

The problem is compounded because many offenders conceal their identity online. They use virtual private networks, encrypted browsers or the dark web to avoid being traced, with the result that investigating agencies may find it difficult to establish the real location of the offender or to collect reliable digital evidence. Even once an accused person has been traced, obtaining information from foreign internet companies is not straightforward. It ordinarily requires assistance from another country through Mutual Legal Assistance Treaties, and that process can take several months.

A further difficulty is that many technology companies store user data on servers located outside India. Indian investigating agencies cannot therefore always access electronic records immediately and must depend on the cooperation of foreign governments and service providers. By the time the required information is received, valuable digital evidence may already have been deleted or altered.

India has entered into Mutual Legal Assistance Treaties with several countries in order to deal with cross-border crime. Delays in sharing electronic evidence nonetheless remain common.

India is not a party to the Council of Europe Convention on Cybercrime and has consistently declined to accede to it, so cross-border assistance continues to rest on bilateral treaty arrangements. In cases involving OCSAE, where digital evidence can disappear within a short time, such delays may seriously affect the investigation and the prospects of a successful prosecution. Given the speed at which digital evidence can be deleted or altered, closer international cooperation and faster mechanisms for sharing electronic evidence are necessary if OCSAE is to be addressed effectively.⁵⁰

B. Identification of child victims

Finding and identifying child victims is often among the hardest parts of investigating Online Child Sexual Abuse and Exploitation. Many children use social media, online games and messaging applications without disclosing their real identity, and offenders take advantage of this. They create fake profiles, pretend to be children or trusted friends, and slowly gain the child's confidence. Once trust has been established they may persuade, pressure or threaten the child into sharing private photographs or videos.

The situation has become more difficult with the rapid growth of artificial intelligence. AI tools can now produce fake images and videos that look almost real, which creates a new challenge for investigating agencies. It may not always be easy to determine whether an image shows a real child or has been generated artificially. Even where no real child was involved in creating such material, its circulation can encourage child sexual exploitation and complicate criminal investigation.⁵¹

A further concern is that many children never report what has happened to them. Some fear that their parents will blame them; others fear embarrassment, social stigma or blackmail by the offender. Because of that fear many cases remain hidden, and the abuse may continue for months before anyone becomes aware of it, giving offenders more time to target other children.⁵²

It is submitted that identifying victims at an early stage is as important as identifying the offender. Better awareness among children, parents, teachers and schools can encourage early reporting, which would help investigating agencies to rescue victims sooner and to prevent further exploitation.

⁵⁰ Convention on Cybercrime, opened for signature at Budapest, November 23, 2001, E.T.S. No. 185, entered into force July 1, 2004, art. 9 and arts. 23-35; see also Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, C.E.T.S. No. 224 (2022). India is not a party to either instrument.

⁵¹ INTERNET WATCH FOUNDATION, *supra* note 33.

⁵² COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2, paras. 81, 113-116.

C. Digital evidence

Digital evidence has become one of the most important elements in the investigation of Online Child Sexual Abuse and Exploitation. In most cases the offence takes place through the internet, so investigators rely on electronic records rather than on traditional evidence. Those records may include chat messages, electronic mail, photographs, videos, IP addresses, mobile telephone data and information stored in cloud accounts. Unlike physical evidence, digital records can be deleted, altered or transferred very quickly, and investigating agencies must therefore act without delay.

Collecting digital evidence is only the first step. It is equally important to preserve it properly so that it can be used in court. Investigators must ensure that electronic records remain unchanged from the time of collection until production at trial, and for that purpose they record metadata, verify files through hash values and maintain a proper chain of custody. Indian courts have insisted on strict compliance with the statutory regime governing electronic records. In *Anvar P.V. v. P.K. Basheer* the Supreme Court held that the statutory certificate is a condition precedent to the admission of an electronic record as secondary evidence, and in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* a three-judge Bench affirmed that position while clarifying that no certificate is required where the original device is itself produced. That requirement now appears in section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024 and re-enacts section 65B of the Indian Evidence Act, 1872 with modifications; the principles laid down in *Anvar* and *Arjun Panditrao* continue to govern.⁵³

Another practical problem is the use of cloud storage. Many internet companies keep user data on servers located outside India, so investigating agencies cannot always obtain electronic records immediately and must often approach service providers and seek assistance from foreign authorities before the required information is shared. That process may take considerable time, during which valuable digital evidence may be lost or become difficult to recover. The increasing use of end-to-end encryption further limits access to communications between offenders and victims. Encryption protects individual privacy, but it also creates practical difficulties in collecting evidence relating to online child sexual exploitation.

Many police officers at the district level still have limited training in digital forensics. Strengthening forensic laboratories, specialised cybercrime units and technical training programmes is therefore essential to improved investigation and successful prosecution.

⁵³ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1; The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63, in force July 1, 2024.

D. AI-generated child sexual exploitation and abuse material

Artificial intelligence has introduced a new dimension to Online Child Sexual Abuse and Exploitation. AI tools are now capable of producing highly realistic sexual images and videos involving children without recourse to traditional photography. These include deepfake images, synthetic abuse material and computer-generated depictions of children. Such content can be created within a few minutes using publicly available software and may closely resemble real children, which makes detection increasingly difficult.

The emergence of AI-generated CSEAM has created legal uncertainty, although the uncertainty is narrower than is sometimes suggested. Indian law does reach synthetic material. Section 2(1)(da) of the POCSO Act, inserted by the amending Act of 2019, extends the statutory definition to a digital or computer-generated image indistinguishable from an actual child and to an image created, adapted or modified so as to appear to depict a child, and section 67B(b) of the Information Technology Act, 2000 separately penalises the creation of text or digital images depicting children in an obscene, indecent or sexually explicit manner. The Supreme Court set out the POCSO definition in terms in *Just Rights for Children Alliance v. S. Harish*. The difficulty lies elsewhere. The statutory threshold is one of resemblance, since the material must be indistinguishable from an actual child or must appear to depict a child. Wholly synthetic imagery of a virtual child that resembles no actual child may therefore fall outside the definition, and that threshold has not yet been tested judicially against the output of current generative models. Nor is there any distinct offence, sentencing framework or forensic standard addressed specifically to AI-generated material. It is these gaps, rather than an absence of statutory coverage, that call for legislative attention.⁵⁴

A further problem is technological. Most online platforms presently rely on hash-matching to detect Child Sexual Exploitation and Abuse Material. That method works well where an image or video has already been identified and its digital fingerprint is available in a reference database. It cannot readily detect new abusive images created with artificial intelligence, because such files do not already exist in the database. Technology companies can therefore no longer depend on hash-matching alone. They also need detection tools capable of recognising newly created abusive content, including deepfake and synthetic material, before it spreads across digital platforms.⁵⁵

⁵⁴ The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), ss. 2(1)(da) and 15; The Information Technology Act, 2000 (Act 21 of 2000), s. 67B(b); *Just Rights for Children Alliance v. S. Harish*, *supra* note 5, para. 48.

⁵⁵ INTERNET WATCH FOUNDATION, *supra* note 33.

Another concern relates to intermediary liability. Social media platforms and internet service providers are expected to remove abusive content promptly, but identifying AI-generated material remains technically challenging. Closer coordination is needed between intermediaries, specialised cybercrime agencies, the Indian Cyber Crime Coordination Centre, the National Cyber Crime Reporting Portal and other child protection authorities if such material is to be detected, reported and removed in time.

The rapid development of artificial intelligence shows that technology is evolving considerably faster than the law. India requires clearer statutory provisions dealing specifically with AI-generated CSEAM, together with improved technological capacity and stronger cooperation between law enforcement agencies and digital platforms.

E. Online grooming

Online grooming is one of the most common methods used by offenders to sexually exploit children. It is a gradual process in which an offender builds trust with a child through social media, online games, messaging applications or other digital platforms. The offender often pretends to be of the same age as the child, offers emotional support, gifts or compliments, and slowly gains the child's confidence. Once trust has been established, the offender may persuade the child to share personal information or intimate photographs, or to participate in sexual activity online.

A major challenge is that grooming usually takes place over a long period and is difficult for parents or teachers to detect. In many cases children do not realise that they are being trapped until it is too late. An offender may behave at first like a friend or offer emotional support, and once the child begins to trust the person, the conversation gradually becomes inappropriate. The offender may then ask for private photographs or videos. If the child refuses, or later attempts to break off communication, those images are often used to threaten or blackmail the child. Many cases of sextortion begin in this way, and the exploitation may continue over a long period.

Indian laws such as the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000 punish many of the offences that result from online grooming. Grooming has not, however, been recognised as a distinct offence under Indian law, although conduct amounting to grooming may be prosecuted as sexual harassment under section 11 of the POCSO Act, which covers repeatedly or constantly following, watching or contacting a child through electronic or digital means, and threatening to use a real or fabricated depiction of the child, both punishable under section 12. Coverage is therefore partial and indirect, and

the police may find it difficult to act at an early stage, before any physical or sexual abuse has taken place.

Preventing online grooming is as important as punishing the offender. Children need to know that they should never share personal information or intimate photographs with strangers on the internet, however friendly the person appears. Parents and teachers also have an important role in guiding children about safe online behaviour. Regular digital safety sessions in schools can make children more aware of online risks and encourage them to report suspicious conversations without shame or fear.⁵⁶

F. Social media platforms

Children spend a considerable amount of time on social media and online gaming platforms. They use applications such as Facebook, Instagram, WhatsApp, Telegram, Snapchat and Discord to talk to friends, attend study groups, share photographs and play games. These platforms offer many benefits, but they have also become places where children may come into contact with offenders.

People involved in Online Child Sexual Abuse and Exploitation often create fake profiles and pretend to be children or trusted adults. Having gained a child's confidence, they may ask for personal information or intimate photographs. In some cases abusive images and videos are shared through private groups or encrypted chats. Features such as disappearing messages, anonymous usernames and live-streaming make it harder for the police to trace offenders. Online games have also become an area of concern, because many conversations begin during gameplay and later move to private messaging applications.

Most technology companies have introduced safety features such as reporting options, parental controls, age restrictions and automated systems for detecting harmful content. These steps have helped to some extent, but they have not solved the problem. Abusive material is not always removed promptly, and children can still create accounts by giving false information about their age. Safety tools alone are therefore not enough.

It is submitted that online platforms need to work more closely with law enforcement agencies and child protection authorities. Prompt removal of Child Sexual Exploitation and Abuse Material, better age verification and faster responses to complaints can make digital platforms safer for children. Parents and teachers should at the same time discuss safe online behaviour

⁵⁶ The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), ss. 11 and 12; COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021)*, *supra* note 2, paras. 81-82, 113-116.

with children regularly, because awareness is often the first step in preventing online exploitation.⁵⁷

G. Encrypted communication

Encrypted messaging applications such as WhatsApp and Signal have changed the way people communicate online. Messages sent through these platforms are protected by end-to-end encryption, which means that only the sender and the recipient can read them. The technology protects users from hacking, data theft and unauthorised access to their private conversations.

Encryption also creates difficulties for criminal investigation. People involved in Online Child Sexual Abuse and Exploitation frequently use encrypted messaging applications to exchange abusive images, videos or messages, precisely because such communications are difficult to access. Even where the police suspect that an offence has been committed, collecting digital evidence may not be straightforward given the level of encryption.

This has produced a continuing debate. Investigating agencies consider that complete encryption slows down investigations into serious offences against children. Privacy experts argue, on the other hand, that weakening encryption would put the personal data of millions of ordinary users at risk. A solution is therefore not simple.

It is submitted that privacy and child safety both deserve protection. Rather than removing encryption altogether, governments and technology companies can work together to develop lawful procedures that assist investigating agencies in genuine cases while protecting the privacy rights of ordinary users. Such an approach is more likely to protect children without compromising the security of everyone using digital platforms.⁵⁸

H. Investigation challenges

Investigating cases of Online Child Sexual Abuse and Exploitation differs considerably from investigating ordinary criminal offences. Police officers have to deal with mobile telephones, computers, cloud storage, social media accounts and other forms of electronic evidence, which requires knowledge of cybercrime and digital forensics. In practice many investigating officers still do not receive sufficient technical training. In several States digital forensic laboratories are limited in number and reports often take months to arrive, and such delays can slow down the entire criminal trial.

⁵⁷ WEPROTECT GLOBAL ALLIANCE, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response* (WeProtect Global Alliance, November 2016); The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1)(b)(ii), 3(2)(b) and 4(4) (notified February 25, 2021).

⁵⁸ *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Coordination between agencies is equally important. A single OCSAE case may involve the local police, cybercrime units, Child Welfare Committees, Special Juvenile Police Units, internet service providers and sometimes foreign authorities. Where these agencies do not share information quickly, the investigation slows and valuable digital evidence may be lost.

Agencies such as the Indian Cyber Crime Coordination Centre, the National Cyber Crime Reporting Portal and the Sahyog Portal, together with internet intermediaries and law enforcement authorities, need to work more closely with one another. Faster reporting of abusive content and its prompt removal can prevent the further circulation of Child Sexual Exploitation and Abuse Material.

It is submitted that improving investigation is not only a matter of enacting stricter laws. It also requires trained investigators, better forensic facilities and technology capable of identifying online abuse at an early stage. If these practical gaps are addressed, the juvenile justice system will be far better placed to respond to offences involving online child sexual exploitation.

I. Victim rehabilitation

The effects of Online Child Sexual Abuse and Exploitation do not disappear once the criminal case is over. For many children the emotional trauma continues long afterwards. They may suffer fear, anxiety, depression or a loss of self-confidence. Some children stop interacting with friends or hesitate to return to school because they feel embarrassed or unsafe. The situation becomes more painful still where abusive photographs or videos remain available on the internet, since every fresh viewing or sharing of such material may renew the child's distress. This repeated harm is commonly described as revictimisation.

Helping the child to recover is as important as punishing the offender, and medical treatment alone is not enough. Many victims need counselling, emotional support from their families, educational assistance and regular guidance from trained professionals. Efforts should also be made to remove abusive content from online platforms so that it cannot continue to circulate. Child Welfare Committees, District Child Protection Units, counsellors and mental health professionals need to work together, because every child may require a different kind of support.

India has created several legal and institutional safeguards for the protection of children. Support services for victims of online sexual exploitation nonetheless remain limited in many parts of the country. Access to trained counsellors is not always available, and long-term rehabilitation often receives less attention than the criminal investigation. It is submitted that greater emphasis should be placed on trauma counselling, digital safety education and rehabilitation programmes that help children to rebuild their confidence. A child who has

experienced online abuse needs care, protection and continued support in order to return to a normal life with dignity and security.⁵⁹

V. RECOMMENDATIONS

India already has laws such as the Juvenile Justice (Care and Protection of Children) Act, 2015, the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000 to protect children from abuse and exploitation. These laws are important, but most of them were enacted before the rapid growth of social media, artificial intelligence and other digital technologies. Investigating agencies today have to deal with online grooming, AI-generated abuse material, encrypted messaging and offences that often cross national borders, which makes investigation and prosecution considerably more difficult than before. Law alone cannot solve the problem. Better coordination among institutions, improved technology, public awareness and international cooperation are equally necessary if children are to be protected in the online environment.

A. Legislative reforms

The existing legal provisions relating to Online Child Sexual Abuse and Exploitation are spread across different enactments, including the POCSO Act, the Information Technology Act, the Bharatiya Nyaya Sanhita and the Juvenile Justice Act. Investigating agencies consequently face uncertainty in deciding which provisions apply in a particular case. A dedicated law dealing specifically with OCSAE would make the legal position clearer and could also lay down uniform rules for investigation, for the collection of digital evidence, for the protection of child victims and for the responsibilities of online platforms.

Artificial intelligence presents a further challenge. Deepfake technology can now produce realistic abusive images of children without using an actual photograph of any child. Existing law reaches such material only through a definition framed in terms of resemblance to an actual child, and it provides no distinct offence, sentencing framework or forensic standard for it. A specific statutory definition of AI-generated Child Sexual Exploitation and Abuse Material, together with a corresponding offence, would remove that uncertainty and assist investigation.

There is also a need for better reporting by digital platforms. Where a platform detects suspected Child Sexual Exploitation and Abuse Material, it should report the matter to the competent authority without unnecessary delay. The United States already operates such a system through

⁵⁹ The Juvenile Justice (Care and Protection of Children) Act, 2015 (Act 2 of 2016), ss. 39-40; The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), ss. 19(5)-(6) and 39; The Protection of Children from Sexual Offences Rules, 2020, r. 9.

the CyberTipline maintained by the National Center for Missing and Exploited Children, to which electronic service providers are required by statute to report.⁶⁰ India can develop a comparable mechanism consistent with its own legal framework.

The responsibilities of intermediaries also need to be stated more clearly. Social media companies, messaging applications and cloud service providers must preserve digital evidence, cooperate with investigating agencies and remove verified abusive material within a reasonable time. Clear legal duties would reduce delay and help investigators to act more quickly.

B. Institutional reforms

Strong laws are important, but they cannot protect children unless the agencies responsible for implementing them are properly equipped. Many cases of Online Child Sexual Abuse and Exploitation involve advanced technology, and investigating such offences requires trained officers and effective coordination between departments.

One useful step would be the creation of a national authority dedicated to Online Child Sexual Abuse and Exploitation. Such a body could bring together work relating to prevention, investigation, victim rehabilitation and research. These responsibilities are at present shared among different agencies, which sometimes leads to delay and poor coordination.

States can also strengthen their response by setting up dedicated cyber child protection units comprising cybercrime investigators, digital forensic experts, psychologists and child welfare officers. Since these cases involve both technology and child protection, a team approach is generally more effective than dealing with each aspect separately.

Digital forensic facilities also need attention. In many States electronic devices are sent to only a few forensic laboratories and examination often takes months, which delays the investigation. More regional forensic laboratories would help to reduce the workload and to speed up the examination of digital evidence.

Training is equally important. Prosecutors and investigating officers should receive regular training on cybercrime, electronic evidence and new technologies, which would help them to handle online child exploitation cases more confidently and to present digital evidence effectively before the courts.

⁶⁰ 18 U.S.C. § 2258A (requiring electronic service providers to report apparent child sexual abuse material to the CyberTipline operated by the NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN).

C. Judicial reforms

Courts have an important role in dealing with cases of Online Child Sexual Abuse and Exploitation. Many child victims have already experienced severe emotional trauma, and where a case continues for years the child may have to relive the experience repeatedly while giving evidence. Prompt disposal of such cases can reduce that hardship and also help to preserve digital evidence before it is lost or altered.

There is also a need for clear procedures governing electronic evidence. Different courts sometimes follow different practices in relation to metadata, forensic reports and the chain of custody. Uniform guidelines would make the trial process smoother and reduce unnecessary disputes about digital evidence.

Judicial officers should receive regular training on technologies such as artificial intelligence, deepfakes, encrypted communication and cryptocurrency. These technologies are changing very quickly, and keeping judges informed will help them to understand technical evidence and to decide such cases with greater confidence.

D. Technological measures

Technology forms part of the problem, and it must therefore form part of the solution. Many organisations now use digital tools to detect Child Sexual Exploitation and Abuse Material before it spreads online. The National Center for Missing and Exploited Children and the Internet Watch Foundation, for example, use technology to identify abusive content and to assist in its removal from online platforms. Similar methods can be adopted more widely in India.

Hash matching and image fingerprinting are among the established methods. Once an abusive image has been assigned a unique digital code, the same image can be detected if it is uploaded again. This saves time and helps to prevent the repeated circulation of known material.

Technology companies can also look for fake accounts and suspicious online activity linked to child exploitation. Such measures should at the same time respect the privacy of users and comply with the law, since the protection of children and the protection of individual rights must go together.

E. Social awareness and community participation

A large number of online child sexual exploitation cases are never reported. Many children are afraid to tell their parents or the police; some feel embarrassed, while others fear that they will not be believed. Spreading awareness is therefore as important as making new laws.

Schools can play a substantial role in prevention. Rather than organising awareness programmes only occasionally, online safety can be built into regular classroom activity. Children should learn how to recognise online grooming, how to keep their personal information safe and how to report suspicious behaviour without fear.

Parents also need better awareness. Many are unfamiliar with the social media applications, online games and messaging platforms that children use every day. Schools, local communities and child protection organisations can hold simple workshops to help parents understand online risks and the use of parental control tools.

Teachers are often the first to notice changes in a child's behaviour. With proper training they can identify warning signs of online abuse and guide children towards counselling or legal help. Non-governmental organisations working for child rights can also support the Government by conducting awareness programmes, assisting victims and helping in their rehabilitation.

F. International cooperation

Online child sexual exploitation is not limited by national borders. In many cases the child is in India, the offender is living in another country and the digital evidence is stored on a foreign server, so that investigation depends on assistance from other States.

India needs quicker access to electronic evidence held outside its territory. Mutual Legal Assistance Treaties already provide a legal process for sharing information, but the procedure is often slow. Since digital evidence can be deleted or altered very quickly, delay may affect the entire investigation, and faster cooperation between States is therefore necessary.

India can also work more closely with international organisations such as INTERPOL, INHOPE, the National Center for Missing and Exploited Children and the Internet Watch Foundation. These organisations regularly assist in tracing Child Sexual Exploitation and Abuse Material, in sharing information with law enforcement agencies and in supporting the removal of abusive content from online platforms. Regular exchange of information, joint investigations and common technical standards would make it easier to deal with offences involving more than one country. Since online child sexual exploitation is a global problem, no State can address it effectively without international cooperation.

VI. CONCLUSION

Children have begun to spend far more time on the internet over the last few years. Online classes after the COVID-19 pandemic, affordable smartphones and easy access to social media have made digital platforms a regular part of everyday life. Children now use the internet not

only for study but also to play games, watch videos and interact with friends. New risks have appeared alongside those benefits. Online Child Sexual Abuse and Exploitation has become a serious concern, because offenders misuse social media, gaming platforms, encrypted messaging applications and even artificial intelligence to target children. Protecting children is therefore no longer confined to the physical world; their safety in the online environment is equally important.

The preceding discussion shows that India already has several laws dealing with offences against children. The Constitution of India, the Juvenile Justice (Care and Protection of Children) Act, 2015, the POCSO Act, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provide legal protection in different ways. Courts have also recognised the changing nature of online offences. The Supreme Court's recent insistence on the expression "child sexual exploitation and abuse material" in place of "child pornography" is one example, and it places the emphasis on the abuse suffered by children rather than treating such material as ordinary pornography.

Several problems persist despite these safeguards. Technology is changing much faster than the law. Deepfake images, AI-generated abuse material, encrypted messaging services and offences involving foreign servers have made investigation more difficult, and many offenders conceal themselves behind fake identities or virtual private networks. The rehabilitation of victims is a further concern, since children often continue to suffer because abusive photographs or videos remain available on the internet long after the criminal case has ended.

Other jurisdictions have responded by building institutions rather than by legislating alone. The United Kingdom, Australia, the United States and the European Union have each invested in specialised agencies, centralised reporting systems, trained investigators and detection technology. A comparative study of those arrangements lies outside the scope of this paper, but their common feature is instructive: statutory reform has been accompanied by institutional capacity. India can draw on that experience while keeping its own constitutional and legal framework in view.

The recommendations set out above concentrate on practical improvement rather than on wholesale legal change. Better digital forensic facilities, specialised cyber child protection units, clearer provisions for AI-generated Child Sexual Exploitation and Abuse Material, stronger digital literacy programmes and closer cooperation with other States can make the existing system more effective. It is submitted that increasing punishment alone will not solve the

problem, and that equal attention must be given to prevention, awareness, prompt investigation and the proper rehabilitation of child victims.

The juvenile justice system is intended not only to punish offenders but also to protect children from further harm, and in the digital world that responsibility has become considerably wider than before. Parents, teachers, schools, courts, investigating agencies, technology companies and civil society all have a part to play. Where these efforts work together, children will be able to use the internet more safely and more confidently. Protecting children online is not a task that ends with the passing of new laws. It is a continuing responsibility, and the legal system must keep pace with changing technology.
