IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 14, May 2026
Impact Factor: 8.2

Cyber Child Sexual Exploitation and Abuse: Challenges in Detection, Digital Evidence Collection, and Legal Enforcement in India

E. Pragadeeswar
1st Year LLM Student, Criminal Law and Criminal Justice Administration, Soel, Tndalu
The Tamilnadu Dr Ambedkar Law University, Chennai

Abstract: *Cyber Child Sexual Exploitation and Abuse (CSEA) has emerged as one of the most serious forms of cybercrime affecting children in the digital era. The rapid growth of internet accessibility, social media platforms, encrypted communication services, online gaming, and digital content-sharing applications has significantly increased the vulnerability of children to online sexual exploitation, grooming, trafficking, pornography, and abuse. In India, the rise in digital penetration and smartphone usage has created new opportunities for offenders to target children through anonymous and cross-border cyber networks, making investigation and prosecution increasingly complex. This study examines the concept, nature, and forms of Cyber Child Sexual Exploitation and Abuse and analyses the major challenges faced in its detection, digital evidence collection, and legal enforcement within the Indian context. The research highlights issues such as underreporting of offences, lack of digital awareness among children and parents, anonymity of offenders, encrypted platforms, jurisdictional limitations, and difficulties in tracing and preserving electronic evidence. It also explores the role of digital forensics in identifying offenders, recovering deleted data, analysing online communications, and maintaining the chain of custody of electronic evidence during criminal investigations.*

The paper further evaluates the effectiveness of the Indian legal framework, including the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, relevant provisions of the Bharatiya Nyaya Sanhita, 2023, and international instruments such as the United Nations Convention on the Rights of the Child. The study identifies gaps in cyber policing, forensic infrastructure, inter-agency coordination, and victim protection mechanisms that hinder effective enforcement. The research concludes that combating CSEA requires a multidimensional approach involving stronger cyber laws, advanced digital forensic capabilities, international cooperation, technological monitoring mechanisms, child awareness programmes, and stricter platform accountability. Effective prevention and enforcement strategies are essential to safeguard children's rights, dignity, privacy, and security in cyberspace..

Keywords: Cyber Child Sexual Exploitation and Abuse (CSEA), Child Sexual Abuse Material (CSAM), cybercrime, online grooming, digital forensics, digital evidence, cyber investigation, child protection, legal enforcement, online child abuse, electronic evidence, cyber security, victim protection, the Protection of Children from Sexual Offences Act, 2012, and the Information Technology Act, 2000

I. INTRODUCTION

The rapid advancement of digital technology and internet accessibility has transformed communication and information sharing across the world. While technological development has created numerous opportunities, it has also led to the emergence of serious cybercrimes affecting vulnerable groups, particularly children. Cyber Child Sexual Exploitation and Abuse (CSEA) refers to the use of digital platforms, online communication networks, and electronic devices for

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 14, May 2026
Impact Factor: 8.2

sexually exploiting, abusing, grooming, or harassing children.[1] the increasing use of social media applications, online gaming platforms, encrypted messaging services, and dark web networks has significantly increased the risk of children becoming victims of online sexual exploitation.

In India, the growth of smartphone usage and affordable internet access has resulted in a sharp rise in cyber-related offences involving children.[2]Offenders often use fake identities, anonymous accounts, and digital platforms to target minors for the creation and circulation of Child Sexual Abuse Material (CSAM), online grooming, trafficking, and extortion. Detecting such offences has become highly challenging due to technological anonymity, encrypted communications, and cross-border cyber operations. Additionally, the collection and preservation of digital evidence require specialised forensic techniques and proper chain-of-custody procedures to ensure admissibility before courts of law.India has introduced several legal measures to combat CSEA, including the Protection of Children from Sexual Offences Act, 2012 (POCSO Act),[3] the Information Technology Act, 2000, and relevant provisions under the Bharatiya Nyaya Sanhita, 2023. Despite these legislative frameworks, challenges such as lack of cyber forensic infrastructure, limited digital awareness, underreporting of offences, jurisdictional barriers, and delays in investigation continue to hinder effective legal enforcement. Therefore, there is an urgent need for stronger cyber policing, international cooperation, digital literacy, and victim protection mechanisms to address the growing threat of Cyber Child Sexual Exploitation and Abuse in India.

Need of the Study

Cyber Child Sexual Exploitation and Abuse (CSEA) has become a rapidly growing cybercrime due to increased internet accessibility, social media usage, and digital communication platforms. Children are increasingly exposed to online grooming, cyber harassment, trafficking, and circulation of Child Sexual Abuse Material (CSAM). Despite the existence of laws such as the POCSO Act, 2012 and the Information Technology Act, 2000, effective detection, investigation, and prosecution of cyber offences against children remain challenging in India. The study is necessary to analyse the emerging nature of CSEA, identify challenges in digital evidence collection and forensic investigation, and examine the effectiveness of existing legal enforcement mechanisms. It also highlights the urgent need for stronger cyber security measures, child protection policies, digital awareness, and coordinated law enforcement strategies.

Significance of the Study

This study is significant because it focuses on the protection of children in cyberspace and examines one of the most serious forms of modern cybercrime. The research contributes to understanding the technological, legal, and investigative challenges involved in combating CSEA in India. It provides insights into the role of digital forensics, cyber policing, and electronic evidence in criminal investigations. The study also helps policymakers, legal professionals, law enforcement agencies, researchers, and educators understand the gaps in the current legal framework and enforcement procedures. Furthermore, the research promotes awareness regarding child online safety and emphasises the importance of international cooperation and victim protection mechanisms in preventing cyber exploitation of children.

Review of Literature

The issue of Cyber Child Sexual Exploitation and Abuse (CSEA) has gained increasing academic and legal attention due to the rapid expansion of digital technology and internet-based communication. Existing literature highlights that children are highly vulnerable to online grooming, cyber harassment, trafficking, and the circulation of Child Sexual Abuse Material (CSAM) through social media platforms, encrypted applications, and dark web networks. Researchers

[1] United Nations Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3

[2] National Crime Records Bureau, Crime in India Report 2024, Ministry of Home Affairs, Government of India

[3] Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code (2012)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

have analysed the technological, legal, and investigative dimensions of cyber offences against children and have emphasised the need for stronger legal enforcement and digital forensic mechanisms.

Susan W. Brenner, in her book *Cybercrime and the Law: Challenges, Issues, and Outcomes*, explains that cybercrime has transformed traditional criminal activities into borderless offences, creating serious challenges for law enforcement agencies in evidence collection and jurisdictional enforcement.[4]The author further discusses how anonymity and encrypted communication technologies make cyber investigations difficult, particularly in cases involving children.

Jonathan Clough, in *Principles of Cybercrime*, examines the nature of online sexual exploitation and explains the growing misuse of internet platforms for grooming and exploitation of minors.[5] The work highlights the importance of digital evidence preservation, cyber policing, and international cooperation in prosecuting cyber offenders.

Studies conducted by the United Nations Office on Drugs and Crime (UNODC) and UNICEF reveal that online child exploitation has significantly increased with the growth of digital communication technologies.[6] These reports identify major challenges such as underreporting of offences, cross-border criminal networks, lack of cyber awareness among parents and children, and inadequate technological infrastructure for investigation.

Indian scholars have also analysed the legal and forensic dimensions of CSEA in India. Aparna Viswanathan, in her work on cyber laws and child protection, discusses the role of the Information Technology Act, 2000 and the Protection of Children from Sexual Offences Act, 2012 in addressing online child abuse.[7]The literature points out that despite comprehensive statutory provisions, implementation gaps continue due to lack of trained cyber forensic experts and delays in digital evidence examination.

Research articles published in journals related to cyber law and digital forensics further emphasise the significance of electronic evidence in prosecuting cyber offenders. Scholars note that proper collection, preservation, and authentication of digital evidence are essential to maintain evidentiary value before courts.[8] Existing studies also recommend specialised cybercrime units, advanced forensic laboratories, international data-sharing mechanisms, and digital literacy programmes to effectively combat Cyber Child Sexual Exploitation and Abuse.

Research Gap

Existing literature on Cyber Child Sexual Exploitation and Abuse (CSEA) mainly focuses on the general concept of cybercrime, online child protection, and legal provisions relating to cyber offences against children. Several studies discuss the technological aspects of online grooming, Child Sexual Abuse Material (CSAM), and digital platforms used by offenders. However, limited research specifically examines the practical challenges faced in India regarding detection, digital evidence collection, forensic investigation, and legal enforcement in CSEA cases. There is also inadequate scholarly analysis on the effectiveness of cyber forensic procedures, inter-agency coordination, cross-border investigation mechanisms, and admissibility of electronic evidence before Indian courts. Therefore, a significant research gap exists in analysing the combined legal, forensic, and enforcement challenges relating to Cyber Child Sexual Exploitation and Abuse in India.

---

[4] Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes* 45–52 (Northeastern University Press 2012)

[5] Jonathan Clough, *Principles of Cybercrime* 311–325 (2nd ed. 2015)

[6] United Nations Office on Drugs and Crime, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (2015); UNICEF, *Child Safety Online: Global Challenges and Strategies* (2021)

[7] Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* 210–220 (2012)

[8] K. Jaishankar, "Cyber Crimes Against Children: Issues and Challenges," 5 Int'l J. Cyber Criminology 45, 49–54 (2011)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 14, May 2026
Impact Factor: 8.2

Research Problem

The rapid increase in internet usage, social media platforms, and digital communication technologies has led to a rise in Cyber Child Sexual Exploitation and Abuse in India. Although India has enacted laws such as the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000, effective detection, investigation, and prosecution of offenders remain difficult. Challenges such as anonymity of offenders, encrypted communication systems, lack of cyber forensic infrastructure, delay in digital evidence examination, jurisdictional barriers, and inadequate technological expertise among law enforcement agencies hinder effective legal enforcement. Consequently, there is a need to critically examine the existing legal and investigative framework relating to Cyber Child Sexual Exploitation and Abuse in India.

Research Questions:

1. What is the nature and scope of Cyber Child Sexual Exploitation and Abuse in India?
2. What are the major challenges faced in the detection and investigation of CSEA offences?
3. How is digital evidence collected, preserved, and analysed in cases involving online child sexual exploitation?
4. How effective are the existing Indian legal frameworks, including the POCSO Act, 2012 and the Information Technology Act, 2000, in addressing CSEA?
5. What are the challenges faced by law enforcement agencies and cyber forensic experts in prosecuting CSEA offences?
6. What legal, technological, and policy measures can be adopted to strengthen child protection and cybercrime enforcement mechanisms in India?

Hypothesis:

1. The increasing use of digital platforms and social media has significantly contributed to the rise of Cyber Child Sexual Exploitation and Abuse (CSEA) in India.
2. Existing legal frameworks in India are insufficient to effectively address the technological and cross-border challenges involved in CSEA offences.
3. Lack of advanced cyber forensic infrastructure and trained investigators negatively affects the detection and prosecution of CSEA cases.
4. Proper collection and preservation of digital evidence play a crucial role in securing convictions in cyber child exploitation cases.
5. Increased digital awareness among children, parents, and educational institutions can reduce the risk of online child sexual exploitation.

Objectives of the Study:

1. To examine the concept, nature, and forms of Cyber Child Sexual Exploitation and Abuse (CSEA).
2. To analyse the increasing impact of digital technology and internet platforms in facilitating online child sexual exploitation.
3. To identify the major challenges involved in the detection and investigation of CSEA offences in India.
4. To evaluate the effectiveness of Indian legal frameworks, including the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000, in combating CSEA.
5. To examine the role of cyber policing, digital forensics, and law enforcement agencies in preventing and prosecuting CSEA offences.
6. To analyse the practical difficulties faced by investigators and courts in handling electronic evidence and cross-border cybercrime cases.
7. To suggest legal, technological, and policy measures for strengthening child protection and cybercrime enforcement mechanisms in India.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

Research Methodology

The present study adopts a doctrinal research methodology. The research is based on secondary sources such as books, journals, research articles, case laws, government reports, and online legal databases. The study analyses the legal and forensic issues relating to Cyber Child Sexual Exploitation and Abuse (CSEA) in India.The research examines important legislations including the Protection of Children from Sexual Offences Act, 2012 (POCSO Act), the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023. International instruments such as the United Nations Convention on the Rights of the Child (UNCRC) are also referred to in the study.

Relevant judicial decisions and legal principles relating to cybercrime, child protection, and electronic evidence are analysed to evaluate the effectiveness of the existing legal framework in combating CSEA in India.

II. Concept of Cyber Child Sexual Exploitation and Abuse (CSEA):

Cyber Child Sexual Exploitation and Abuse (CSEA) refer to the use of digital technologies, internet platforms, social media applications, and electronic communication systems to sexually exploit, abuse, harass, or groom children.[9] It includes activities such as online grooming, circulation of Child Sexual Abuse Material (CSAM), live-streaming of abuse, cyber stalking, online trafficking, and sexual extortion through digital platforms. Offenders often use fake identities, anonymous accounts, and encrypted communication systems to target minors and exploit their vulnerability.[10]

CSEA has emerged as a serious form of cybercrime due to rapid technological advancement and increased internet accessibility. The offence affects the physical, mental, and emotional well-being of children and violates their dignity, privacy, and fundamental rights.[11] In India, legislations such as the Protection of Children from Sexual Offences Act, 2012 (POCSO Act) and the Information Technology Act, 2000 provide legal measures to address online child exploitation and cyber offences against children.[12]

Concept of Digital Evidence and Collection:

Digital evidence collection refers to the process of identifying, securing, preserving, extracting, and documenting electronic data for use in criminal investigations and judicial proceedings.[13] Digital evidence may include emails, chat records, social media communications, photographs, videos, metadata, browsing history, IP addresses, and data stored in computers, mobile phones, or cloud platforms.

In Cyber Child Sexual Exploitation and Abuse cases, digital evidence plays a crucial role in identifying offenders, tracing online activities, recovering deleted files, and proving criminal conduct before courts of law.[14] Proper handling and preservation of electronic evidence are essential to maintain authenticity, integrity, and admissibility during trial proceedings. Investigating agencies use digital forensic techniques such as forensic imaging, data recovery, metadata analysis, and cyber tracking while maintaining the chain of custody.[15] In India, the Bharatiya Sakshya Adhiniyam, 2023 and the Information Technology Act, 2000 govern the admissibility and management of electronic evidence.

---

[9] Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes* 45–48 (Northeastern University Press 2012)

[10] Jonathan Clough, *Principles of Cybercrime* 311–320 (2nd ed. 2015)

[11] UNICEF, *Child Safety Online: Global Challenges and Strategies* (2021)

[12] Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code (2012); Information Technology Act, No. 21 of 2000, India Code (2000)

[13] Eoghan Casey, *Digital Evidence and Computer Crime* 7–15 (3rd ed. 2011)

[14] K. Jaishankar, "Cyber Crimes Against Children: Issues and Challenges," 5 Int'l J. Cyber Criminology 45, 49–54 (2011)

[15] Matthew G. Kirschenbaum, *Mechanisms: New Media and the Forensic Imagination* 120–126 (2008)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

III. Legal Framework Relating to Cyber Child Sexual Exploitation and Abuse (CSEA)

International Legal Framework

The international legal framework relating to Cyber Child Sexual Exploitation and Abuse (CSEA) focuses on the protection of children from sexual abuse, exploitation, trafficking, and online victimisation. The United Nations Convention on the Rights of the Child (UNCRC), 1989 is one of the most important international instruments protecting children from all forms of sexual exploitation and abuse. Article 19 of the Convention obligates States to protect children from physical or mental violence, abuse, and exploitation, while Article 34 specifically requires States to prevent child sexual exploitation and pornography.[16]

The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2000 further criminalises child pornography, online exploitation, and trafficking of children through digital platforms.[17] The Budapest Convention on Cybercrime, 2001 is another important international treaty addressing cyber offences and electronic evidence collection. Article 9 of the Convention specifically deals with offences related to child pornography committed through computer systems and online communication networks.[18]

International organisations such as UNICEF and the United Nations Office on Drugs and Crime (UNODC) have also issued guidelines and strategies for combating online child exploitation, digital abuse, and cyber-enabled trafficking of children.

Indian Legal Framework

India has enacted several legislations to address Cyber Child Sexual Exploitation and Abuse and related cyber offences against children. The Protection of Children from Sexual Offences Act, 2012 (POCSO Act) is the primary legislation dealing with child sexual abuse and exploitation. Section 13 criminalises the use of children for pornographic purposes, while Sections 14 and 15 prescribe punishment for storage, distribution, and possession of child pornographic material.[19]

The Information Technology Act, 2000 contains specific provisions addressing online obscenity and sexually explicit material involving children. Section 67B of the Act criminalises publishing, browsing, downloading, advertising, promoting, or transmitting material depicting children in sexually explicit acts through electronic form.[20]The Act also empowers authorities to investigate cyber offences and regulate electronic evidence.

The Bharatiya Nyaya Sanhita, 2023 includes provisions relating to trafficking, sexual offences, and exploitation of minors. Further, the Bharatiya Sakshya Adhiniyam, 2023 provides legal recognition and admissibility to electronic evidence in judicial proceedings, which is essential in prosecuting CSEA offences involving digital communication and online platforms.

The Indian legal framework is further supported by specialised cybercrime cells, digital forensic laboratories, and reporting mechanisms established by the Government of India to strengthen child protection and cybercrime enforcement.

Constitutional Protection Against Cyber Child Sexual Exploitation and Abuse in India

The Constitution of India provides several fundamental rights and constitutional safeguards for the protection of children against exploitation, abuse, and violation of dignity, including offences committed through cyberspace. These constitutional provisions form the foundation for child protection laws and cybercrime legislation in India.

---

[16] United Nations Convention on the Rights of the Child arts. 19 & 34, Nov. 20, 1989, 1577 U.N.T.S. 3

[17] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227

[18] Convention on Cybercrime art. 9, Nov. 23, 2001, E.T.S. No. 185 (Budapest Convention)

[19] Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 13–15, India Code (2012)

[20] Information Technology Act, No. 21 of 2000, § 67B, India Code (2000)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

Article 14 of the Constitution guarantees equality before law and equal protection of laws to all persons, including children.[21]Article 15(3) empowers the State to make special provisions for women and children to ensure their protection and welfare.[22] Article 21 guarantees the right to life and personal liberty, which includes the right to live with dignity, privacy, safety, and protection from exploitation.[23] Cyber Child Sexual Exploitation and Abuse violates the dignity, privacy, and mental well-being of children protected under Article 21.

Article 21A guarantees the right to education for children between the ages of six and fourteen years, promoting a safe and secure environment for child development.[24]Article 23 prohibits trafficking in human beings and forced labour, which indirectly includes online child trafficking and exploitation through digital platforms.[25] Article 24 prohibits employment of children in hazardous occupations and protects them from exploitation and abuse.[26]

The Directive Principles of State Policy also impose duties upon the State to protect children. Article 39(e) directs the State to ensure that children are not abused or forced into unsuitable activities, while Article 39(f) requires the State to provide opportunities for healthy development and protection against exploitation and moral abandonment.[27] Further, Article 45 promotes early childhood care and education for children.

The constitutional framework, along with legislations such as the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000, plays an important role in protecting children from cyber sexual exploitation and abuse in India.

IV. Criminal Liability, Detection and Digital Evidence Collection in Cyber Child Sexual Exploitation and Abuse (CSEA)

Cyber Child Sexual Exploitation and Abuse (CSEA) has emerged as one of the most serious forms of cybercrime affecting children in the digital age. The internet, social media platforms, encrypted messaging applications, cloud storage services, and dark web networks have enabled offenders to groom, exploit, abuse, and disseminate Child Sexual Abuse Material (CSAM) on an unprecedented scale. In India, criminal liability for such offences is imposed through a combination of child protection laws, cybercrime legislation, and general criminal law provisions. The Protection of Children from Sexual Offences Act, 2012 (POCSO Act) criminalizes the use of children for pornographic purposes and penalizes the storage, possession, transmission, and distribution of child sexual abuse material. Sections 13, 14, and 15 of the Act specifically address offences relating to child pornography and online sexual exploitation.[28]Additionally, Section 67B of the Information Technology Act, 2000 makes it a punishable offence to publish, transmit, browse, download, advertise, or facilitate access to material depicting children in sexually explicit acts through electronic means.[29] Depending on the nature of the offence, provisions relating to criminal conspiracy, trafficking, extortion, sexual harassment, and organized crime under the Bharatiya Nyaya Sanhita, 2023 may also be invoked. Thus, individuals who create, possess, distribute, or facilitate the circulation of CSAM through digital platforms can incur substantial criminal liability under Indian law.

The detection of Cyber Child Sexual Exploitation and Abuse presents significant challenges because offenders frequently exploit technological tools to conceal their identities and activities. Criminals often use encrypted

[21] INDIA CONST. art. 14
[22] INDIA CONST. art. 15(3)
[23] INDIA CONST. art. 21
[24] INDIA CONST. art. 21A
[25] INDIA CONST. art. 23
[26] INDIA CONST. art. 24
[27] INDIA CONST. art. 39(e)–(f)
[28] Protection of Children from Sexual Offences Act, No. 32 of 2012, s- 13–15 (India)
[29] Information Technology Act, No. 21 of 2000, s 67B (India)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

communication platforms, anonymous email accounts, virtual private networks (VPNs), proxy servers, cryptocurrency transactions, and dark web forums to evade law enforcement surveillance. Furthermore, victims may be reluctant to report incidents due to fear, social stigma, or manipulation by offenders. Nevertheless, Indian authorities employ several mechanisms to detect CSEA offences, including cybercrime monitoring, artificial intelligence-based content recognition systems, digital surveillance, cyber tip lines, and complaints received through the National Cyber Crime Reporting Portal. The mandatory reporting obligation contained in Section 19 of the POCSO Act further strengthens detection by requiring any person who becomes aware of child sexual abuse offences to report them to the appropriate authorities.[30] Failure to report such offences may itself attract legal consequences. The Supreme Court of India has also emphasized the need for proactive identification and removal of online child sexual abuse content and directed authorities to strengthen monitoring and enforcement mechanisms against digital child exploitation networks.[31]

Digital evidence constitutes the foundation of investigation and prosecution in CSEA cases because most offences are committed, facilitated, or documented through electronic devices and online communication systems. Digital evidence may include photographs, videos, chat messages, emails, browsing history, metadata, cloud storage records, social media communications, IP address logs, location data, and records of financial transactions associated with exploitation activities. Investigators must collect such evidence in accordance with established forensic procedures to ensure its integrity and admissibility before courts. The process generally begins with the identification and seizure of digital devices such as computers, smartphones, tablets, hard drives, and storage media. Thereafter, forensic experts create exact digital copies, known as forensic images, to preserve the original evidence from alteration. Investigators then analyse the copied data to recover deleted files, identify communication patterns, trace user activity, examine metadata, and establish links between suspects and victims. Maintaining an unbroken chain of custody throughout the investigation is essential to prevent allegations of tampering and to ensure the reliability of evidence during trial.

The legal admissibility of electronic evidence in India is governed by the Bharatiya Sakshya Adhiniyam, 2023. Sections 63 and 65 recognize electronic records as documentary evidence and prescribe the conditions under which such records may be admitted before courts.[32] Compliance with these statutory requirements is crucial because procedural deficiencies may undermine the evidentiary value of digital records. Cyber forensic laboratories, CERT-In, specialized cybercrime units, and international law enforcement agencies frequently assist investigators in preserving and analysing electronic evidence, particularly in cases involving transnational criminal networks. However, investigators continue to face numerous challenges, including end-to-end encryption, disappearing messages, jurisdictional barriers, limited access to foreign servers, lack of specialized forensic expertise, and the rapid deletion or modification of electronic records. These challenges often delay investigations and complicate the prosecution of offenders. Consequently, effective enforcement against CSEA requires stronger technological capabilities, specialized training for investigators, enhanced international cooperation, and robust digital forensic infrastructure to ensure that perpetrators are successfully identified, prosecuted, and punished.

V. Important Case Laws on Cyber Child Sexual Exploitation and Abuse (CSEA)

1. In Re: Prajwala Letter Petition v. Union of India, (2015) 8 SCC 735

Facts

The case originated from a letter addressed to the Supreme Court highlighting the alarming circulation of rape videos, child pornography, and sexually exploitative content on the internet. The letter pointed out that online platforms were being used to disseminate Child Sexual Abuse Material (CSAM) and sought judicial intervention to curb such activities. Treating the letter as a Public Interest Litigation, the Supreme Court took suo motu cognizance of the matter.

Issues

[30] Protection of Children from Sexual Offences Act, No. 32 of 2012, s 19 (India)

[31] *In Re: Prajwala Letter Petition v. Union of India*, (2015) 8 SCC 735

[32] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 63–65 (India)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

1. Whether the Government of India and law enforcement agencies were taking adequate measures to prevent the circulation of child pornography and sexually abusive content online.
2. Whether internet intermediaries and service providers could be directed to identify and remove such content.
3. Whether a coordinated mechanism was required for reporting and blocking child sexual abuse material.

Judgment

The Supreme Court directed the Central Government, law enforcement agencies, and internet intermediaries to establish effective mechanisms for identifying, reporting, removing, and blocking child sexual abuse content available on digital platforms. The Court emphasized that the protection of children from sexual exploitation is a constitutional obligation and directed authorities to strengthen cyber monitoring and enforcement measures against online child abuse networks. The decision remains one of the most significant judicial interventions concerning online child sexual exploitation in India.[33]

2. Sharat Babu Digumarti v. Government (NCT of Delhi), (2017) 2 SCC 18

Facts

The accused was associated with the operation of an online platform through which obscene and sexually explicit material was circulated electronically. The prosecution initiated proceedings under both the Information Technology Act, 2000 and provisions of the Indian Penal Code. The case involved the question of liability for the transmission of objectionable content through electronic means.

Issues

1. Whether offences involving electronic transmission of obscene material should be prosecuted under the Information Technology Act or general criminal law.
2. Whether special provisions of the IT Act override general penal provisions.

Judgment

The Supreme Court held that where the Information Technology Act specifically deals with electronic publication or transmission of objectionable content, the provisions of the IT Act would prevail over general penal provisions. The judgment strengthened the application of Section 67B of the Information Technology Act in cases involving online child sexual abuse material and electronic sexual exploitation.[34]

3. Alakh Alok Srivastava v. Union of India, W.P. (C) No. 1303 of 2019

Facts

The petitioner sought directions from the Supreme Court regarding the increasing availability of child pornography on online platforms and social media applications. The petition highlighted the ease with which child sexual abuse material could be accessed and shared through digital technologies.

Issues

1. Whether internet intermediaries should be obligated to remove child pornography promptly.
2. Whether technological mechanisms should be adopted to prevent the circulation of CSAM.
3. Whether stricter regulatory measures were necessary to protect children online.

Judgment

The Supreme Court directed the Government of India and intermediaries to take effective measures for detecting, removing, and reporting child sexual abuse material. The Court stressed the need for advanced technological tools, cooperation with international agencies, and stronger enforcement against offenders involved in online child exploitation.[35]

[33] *In Re: Prajwala Letter Petition v. Union of India*, (2015) 8 SCC 735

[34] *Sharat Babu Digumarti v. Government (NCT of Delhi)*, (2017) 2 SCC 18

[35] *Alakh Alok Srivastava v. Union of India*, W.P. (C) No. 1303 of 2019 (Sup. Ct. India)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

4. X v. State of Maharashtra, 2024 SCC OnLine Bom 563 (Related to Possession of Child Pornography)

Facts

The accused was found in possession of digital material containing child sexual abuse content stored on electronic devices. The issue before the Court concerned whether mere possession or downloading of such material constituted an offence under the POCSO Act and the Information Technology Act.

Issues

1. Whether possession of child sexual abuse material without proof of transmission constitutes an offence.
2. Whether downloading and storing such content attracts criminal liability.

Judgment

The Court held that possession, storage, and access to child sexual abuse material can amount to criminal conduct under the POCSO Act and the Information Technology Act. The judgment emphasized that digital possession itself contributes to the exploitation of children and cannot be treated as a victimless act.[36]

5. Just Rights for Children Alliance v. Union of India, 2024 SCC Online SC 2965

Facts

The petition concerned the increasing circulation of child pornography and the inadequacy of existing legal responses to online child sexual abuse material. The petitioners sought stronger interpretation and enforcement of POCSO provisions relating to digital exploitation.

Issues

1. Whether possession and viewing of child sexual abuse material should be criminalized.
2. Whether the term "child pornography" should be replaced with a more victim-centred terminology.
3. Whether stronger obligations should be imposed on digital platforms.

Judgment

The Supreme Court clarified that possession, storage, viewing, and dissemination of child sexual abuse material are punishable offences under the POCSO Act and the Information Technology Act. The Court recommended the use of the term "Child Sexual Exploitative and Abuse Material (CSEAM)" instead of "child pornography" to better reflect the exploitative nature of the offence. The judgment significantly strengthened the legal framework against online child exploitation in India.[37]

VI. Challenges in Detection, Digital Evidence Collection, and Legal Enforcement of Cyber Child Sexual Exploitation and Abuse (CSEA) in India

Cyber Child Sexual Exploitation and Abuse (CSEA) pose significant challenges to law enforcement agencies, digital forensic investigators, policymakers, and judicial institutions in India. One of the foremost challenges is the **anonymity of offenders in cyberspace**. Perpetrators frequently use encrypted messaging applications, virtual private networks (VPNs), anonymous accounts, proxy servers, and the dark web to conceal their identities and locations. This anonymity makes it difficult for investigators to identify offenders and establish jurisdiction, particularly when crimes involve multiple countries and cross-border digital platforms.[38]

Another major challenge is the **rapid dissemination and persistence of Child Sexual Abuse Material (CSAM)** on digital platforms. Once such material is uploaded online, it can be copied, shared, downloaded, and redistributed across numerous websites and applications within minutes. Even after the removal of content from one platform, identical material may reappear elsewhere, making complete eradication extremely difficult. The global nature of internet infrastructure further complicates efforts to remove abusive content permanently.[39]

---

[36] *X v. State of Maharashtra*, 2024 SCC OnLine Bom 563

[37] *Just Rights for Children Alliance v. Union of India*, 2024 SCC OnLine SC 2965

[38] United Nations Office on Drugs and Crime, *Global Report on Trafficking in Persons* (2024)

[39] INTERPOL, *International Child Sexual Exploitation Database (ICSE) Report* (2023)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

The **collection and preservation of digital evidence** present substantial difficulties in CSEA investigations. Electronic evidence is highly volatile and can be altered, deleted, encrypted, or remotely destroyed by offenders. Investigators must follow strict forensic procedures to maintain the integrity and admissibility of evidence. Failure to preserve metadata, maintain chain of custody, or obtain proper certification for electronic records may weaken the prosecution's case and affect judicial outcomes.[40]

A further challenge is the increasing use of **end-to-end encryption technologies** by communication platforms. While encryption enhances privacy and cybersecurity, it also creates obstacles for law enforcement agencies attempting to access communications related to child exploitation offences. Investigators often encounter difficulties in obtaining critical evidence such as chat histories, images, videos, and user information, particularly when service providers are located outside India and are governed by foreign legal regimes.[41]

The **lack of specialized cyber forensic infrastructure and trained personnel** remains another significant concern. Although India has established cybercrime units and forensic laboratories, many states continue to face shortages of digital forensic experts, advanced investigative tools, and technical resources. The increasing volume and complexity of cybercrime cases frequently result in delays in forensic analysis, which may adversely affect the quality of investigations and prosecutions.[42]

Victim-related challenges also hinder effective enforcement. Children subjected to online sexual exploitation may be reluctant to report offences because of fear, shame, social stigma, threats from offenders, or lack of awareness regarding available legal remedies. In many instances, victims are manipulated through grooming techniques and may not immediately recognize that they are being exploited. Consequently, delayed reporting often results in loss of evidence and reduced opportunities for timely intervention.[43]

Jurisdictional and international cooperation issues further complicate the enforcement of laws against CSEA. Offenders, victims, internet service providers, cloud storage servers, and digital platforms may be located in different countries. Obtaining electronic records from foreign jurisdictions often requires Mutual Legal Assistance Treaties (MLATs), diplomatic cooperation, and compliance with diverse legal standards, resulting in procedural delays and evidentiary challenges.[44]

Finally, despite the existence of legal provisions under the POCSO Act, the Information Technology Act, and the Bharatiya Nyaya Sanhita, enforcement agencies continue to face challenges relating to technological advancements, emerging forms of online exploitation, cryptocurrency-based transactions, artificial intelligence-generated sexual content, and evolving cybercrime methodologies. These developments require continuous legislative reforms, capacity building, international collaboration, and technological innovation to ensure effective protection of children in the digital environment.[45]

VII. Suggestions

1. Strengthen Cyber Laws – Amend and update the POCSO Act, Information Technology Act, and Bharatiya Nyaya Sanhita to address emerging cyber threats such as AI-generated child sexual abuse material, deepfakes, and dark web offences.
2. Enhance Digital Forensic Infrastructure – Establish advanced cyber forensic laboratories in all states and equip them with modern investigation tools.

[40] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, S63–65 (India)
[41] Information Technology Act, No. 21 of 2000, S67B (India)
[42] National Crime Records Bureau, *Crime in India Report* (latest available edition)
[43] Protection of Children from Sexual Offences Act, No. 32 of 2012, § 19 (India)
[44] United Nations, *Convention against Transnational Organized Crime*, Nov. 15, 2000, 2225 U.N.T.S. 209
[45] *Just Rights for Children Alliance v. Union of India*, 2024 SCC OnLine SC 2965

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

3. Specialized Training for Law Enforcement – Provide regular training to police officers, prosecutors, judges, and forensic experts on cybercrime investigation and digital evidence handling.
4. Use Artificial Intelligence and Advanced Technology – Deploy AI-based tools, image-hashing technologies, and automated content detection systems to identify and remove CSAM from online platforms.
5. Strengthen Monitoring of Online Platforms – Require social media companies, internet service providers, and intermediaries to proactively detect, report, and remove child sexual abuse content.
6. Improve International Cooperation – Enhance collaboration with foreign governments, INTERPOL, and international organizations for cross-border investigations and evidence sharing.
7. Promote Mandatory Reporting – Increase awareness regarding the reporting obligations under Section 19 of the POCSO Act and encourage timely reporting of offences.
8. Child-Friendly Reporting Mechanisms – Establish confidential and accessible reporting channels for children and their guardians.
9. Victim Rehabilitation and Support – Provide psychological counselling, legal aid, rehabilitation services, and compensation to victims of cyber sexual exploitation.
10. Digital Literacy and Cyber Safety Education – Introduce cyber safety awareness programs in schools and educational institutions to educate children about online risks and safe internet practices.
11. Public Awareness Campaigns – Conduct nationwide awareness campaigns on cyber grooming, sextortion, online abuse, and reporting mechanisms.
12. Strengthen Data Sharing and Coordination – Create a centralized national database for information sharing among law enforcement agencies, child protection authorities, and cybercrime units.
13. Fast-Track Investigation and Trial – Establish specialized cybercrime and POCSO courts to ensure speedy investigation and disposal of CSEA cases.

VIII. Conclusion

Cyber Child Sexual Exploitation and Abuse (CSEA) is one of the most serious challenges in the digital era. The rapid growth of the internet and digital technologies has increased opportunities for offenders to exploit children online. India has enacted laws such as the POCSO Act, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023 to address these offences. However, the detection and investigation of CSEA remain difficult due to anonymity, encryption, and cross-border cybercrime. Digital evidence plays a crucial role in identifying offenders and securing convictions. Proper collection, preservation, and analysis of electronic evidence are essential for successful prosecution. Law enforcement agencies also face challenges such as inadequate forensic resources and jurisdictional barriers. Victims often suffer severe psychological and emotional harm, making rehabilitation and support services necessary. Public awareness and digital literacy are important in preventing online exploitation. Parents, schools, and communities must actively participate in safeguarding children online. Technology companies should strengthen content monitoring and reporting mechanisms. International cooperation is also essential to combat transnational exploitation networks. Continuous training of investigators and judicial officers can improve enforcement. A coordinated approach involving legal, technological, and social measures is necessary. Therefore, strengthening child protection mechanisms and cybercrime enforcement is crucial to ensuring a safe digital environment for children.

REFERENCES AND BIBLIOGRAPHY

Statutes

1. Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code (2012).
2. Information Technology Act, No. 21 of 2000, India Code (2000).
3. Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).
4. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (2023).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 14, May 2026 Impact Factor: 8.2

5. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023).
6. Constitution of India arts. 14, 15(3), 21, 23, 39(e), 39(f).

Cases

1. *In Re: Prajwala Letter Petition v. Union of India*, (2015) 8 S.C.C. 735 (India).
2. *Sharat Babu Digumarti v. Gov't (NCT of Delhi)*, (2017) 2 S.C.C. 18 (India).
3. *Alakh Alok Srivastava v. Union of India*, W.P. (C) No. 1303 of 2019 (India).
4. *Just Rights for Children All. v. Union of India*, 2024 SCC OnLine SC 2965 (India).
5. *Avnish Bajaj v. State (NCT of Delhi)*, 150 (2008) D.L.T. 769 (Del. H.C.).
6. *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004 (Chennai Dist. Ct. 2004).

International Conventions and Instruments

1. United Nations, Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.
2. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227.
3. United Nations, United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.
4. United Nations, Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Nov. 15, 2000, 2237 U.N.T.S. 319.
5. International Labour Organization, Convention No. 182 Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour, June 17, 1999.

Reports and Publications

1. National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Gov't of India 2024).
2. National Commission for Protection of Child Rights, *Manual on Safety and Security of Children in Cyberspace* (2022).
3. United Nations Office on Drugs and Crime, *Global Report on Trafficking in Persons* (2024).
4. INTERPOL, *International Child Sexual Exploitation Database (ICSE) Report* (2023).
5. UNICEF, *Child Online Protection and Digital Safety Report* (2023).
6. Internet Watch Foundation, *Annual Report 2024* (2024).

Books

1. Talwant Singh, *Cyber Law & Information Technology* (3d ed. 2022).
2. Karnika Seth, *Computers, Internet and New Technology Laws* (3d ed. 2021).
3. Justice Yatindra Singh, *Cyber Laws* (6th ed. 2022).
4. Farooq Ahmad, *Cyber Law in India: Law on Internet* (4th ed. 2020).
5. Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce and Consumer Protection* (2019).

DOI: 10.48175/568