
DIGITAL ABUSE OF CHILDREN IN INDIA: EMERGING CHALLENGES AND THE EFFICACY OF THE POCSO ACT, 2012

Robin Bharti, Research Scholar, Department of Law, Kurukshetra University Kurukshetra, Haryana, India

Dr. Pooja, Assistant Professor, Department of Law, Kurukshetra University Kurukshetra, Haryana, India.

ABSTRACT

The high speed of the growth of digital technologies has changed the way children communicate, learn, socialise and get access to information. Nevertheless, greater exposure to the digital world has also led to new prospects of abusing, exploiting and harassing children. Digital abuse can be done in a number of ways such as on-line grooming, cyber sexual harassment, sextortion, distribution of child sexual abuse content, image-based abuse, impersonation and technology-based sexual exploitation. Anonymity of offenders, the high rate of distribution of digital contents, secure communication, cross-border aspect of online crimes as well as the emergence of new technologies like artificial intelligence and deepfakes have also increased the challenge of offering protection to children in the online world. The POCSO Act has played a significant role in providing a statutory framework to protect the child against sexual offences in India via the Protection of Children against Sexual Offences Act, 2012 (POCSO act) that covers various forms of sexual abuse that are related to technology. Nevertheless, it is the dynamism of digital abuse that begs the question of the validity and online applicability of the current law.

This paper discusses what digital abuse of children involves and what are the dimensions of this issue in India and critically discusses how effective the POCSO Act, 2012 has so far been in tackling it. It provides an analysis of the provisions of the POCSO Act as well as other applicable laws, including the Information Technology Act, 2000, Information Technology Rules, 2021, Bharatiya Nyaya Sanhita, 2023 and Digital Personal Data Protection Act, 2023. This paper also analyzes the judicial practice, investigative issues, the evidentiary challenges, institutional procedures and the roles of digital platforms in deterring and addressing technology-based abuse. Specific consideration is given to the new challenges of artificial intelligence, deepfakes and the growing amount of harmful online content. The paper will take a socio-legal and doctrinal approach to find out the gaps between legal

safeguarding and application in reality. It postulates that even though the POCSO Act has become an important protective tool, its usefulness in the online space relies upon technical capacity, organized enforcement, child-focused practices, internet literacy, and internet accountability and ongoing legal evolution. The paper ends by recommending actions to improve the child protection system in India to deal with the quickly developing types of digital abuse.

Keywords: Digital Abuse, Children, POCSO Act, Online Grooming, Child Sexual Abuse Material, Cybercrime, Deepfakes, Child Protection

1. Introduction

The sudden evolution of new digital technology has changed the modes of communication, learning and interaction among children. Social media, messaging apps and online learning platforms, online gaming, smartphones have all become relevant aspects of the lives of children. On the one hand, these technologies offer educational and social opportunities, on the other hand, they establish new opportunities of exploitation, harassment and sexual abuse. Through digital abuse, as opposed to traditional abuse, criminals have a chance to commit their crimes at a distance and remain anonymous and the nature of harmful content can be duplicated and distributed across national boundaries, quickly.¹

Online grooming, cyber sexual harassment, sextortion, and child sexual abuse content, image-based abuse, and impersonation and other types of technology-mediated exploitation are examples of digital abuse. The issue has been worsened by the development of both artificial intelligence and the deepfake technology, allowing one to create a convoluted or falsified sexual content with the use of children. These changes present a new array of concerns with regard to privacy, dignity, digital evidence and criminal responsibility.²

The Protection of children against sexual offences act, 2012 (POCSO act) is the main specialised law in India guarding children against sexual offences.³ The specifics in its provisions concerning sexual harassment and the use of children to obtain pornographic content is especially applicable in digital abuse. The broader legal framework is contributed to by Information technology laws; Information Technology Act, 2000,⁴ Information Technology

¹ Karnika Seth, *Protection of Children on Internet* (LexisNexis, New Delhi, 2013), pp. 1–15.

² Poonam Mishra & Roshni Srivastava, “Digital Sexual Exploitation of Children: Analysing POCSO Provisions on Pornography and Online Abuse in India,” *Indian Journal of Legal Review*, Vol. 6, Issue 4, 2026, pp. 324–332.

³ The Protection of Children from Sexual Offences Act, 2012, Sections 11–15.

⁴ The Information Technology Act, 2000, Section 67B.

Rules, 2021 and Bharatiya Nyaya Sanhita, 2023.⁵ also contribute to the broader legal framework.⁶

In spite of these provisions, the anonymity of offenders, encryption, transnational crimes, the challenges in electronic evidence-keeping and underreporting by minors are the reasons why the protection process has not been effective. New technologies like AI and deepfakes present even more to prove the inability of the laws that are already in place.

It is against this backdrop that the current research study analyzes digital harassment of children in India particularly in reference to the effectiveness of POCSO Act, 2012. It examines key types of online abuse, the applicable laws, courts and real-life enforcement issues. The research claim that having POCSO as a vital legal framework is a crucial step in ensuring protection, yet technological readiness, specialised investigation, child-friendly reporting processes, and continuous legal development are also essential.

2. Concept and Forms of Digital Abuse of Children

2.1 Meaning of Digital Abuse

Digital abuse of children is defined as actions that are harmful to children via digital devices, electronic communications or the internet. It can have an impact on the safety, dignity, privacy and the psychological well-being of a child. The perpetrator can also be able to connect, control the child, gain access to personal information or provide some dangerous content which is use of technology. Digital abuse can be carried out even without the need to have any physical contact in the face of each other as compared to physical abuse.⁷

2.2 Online Grooming

Online grooming is an act of building trust or emotional relationship with a child online with the intention of engaging in sexual exploitation towards the same. Also attackers can pose as friends or peers and build up slowly soliciting personal information, photos, video dialogue or in-person visits. It is gradual in nature; hence it is hard to determine and emphasizes the need

⁵ The Bharatiya Nyaya Sanhita, 2023.

⁶ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

⁷ Karnika Seth, *Protection of Children on Internet* (LexisNexis, New Delhi, 2013), pp. 1–15.

of digital awareness among children and parents.⁸

2.3 Cyber Sexual Harassment

Cyber sexual harassments involve unsolicited sexual texts, nude pictures, sexual remarks, persistent offers of intimate contents and threats of violence on the Internet. Since digital communication can happen at all times and on many platforms, such behavior might result in ongoing fear and insecurity by the child.⁹

2.4 Sextortion

Cyber sexual harassments involve unsolicited sexual texts, nude pictures, sexual remarks, persistent offers of intimate contents and threats of violence on the Internet. Since digital communication can happen at all times and on many platforms, such behavior might result in ongoing fear and insecurity by the child.¹⁰

2.5 Child Sexual Abuse Material

Manufacturing, possession, transmission and distribution of content that portrays children as being involved in sexually explicit scenarios are severe types of digital exploitation. Through digital technology, one can easily disseminate and access such material several times, leading to ongoing victimisation of the child.

2.6 Image-Based Abuse and Impersonation

The intimate or sexualised images of children can be received with the help of lies, formation or without permission and later be distributed by online platforms. Likewise, criminals can also create a prank profile or identity of a person they trust to win over a child to obtain personal or sexually explicit content.¹¹

2.7 AI-Generated and Deepfake Abuse

There is an artificial intelligence and deepfake technology that can be used to produce

⁸ Poonam Mishra & Roshni Srivastava, "Digital Sexual Exploitation of Children: Analysing POCSO Provisions on Pornography and Online Abuse in India," *Indian Journal of Legal Review*, Vol. 6, Issue 4, 2026, pp. 324–332.

⁹ Karnika Seth, *Cyber Laws and Information Technology* (LexisNexis, New Delhi, 2016), pp. 285–292.

¹⁰ National Crime Records Bureau, *Crime in India 2023*, Ministry of Home Affairs, Government of India, New Delhi, 2024.

¹¹ R.K. Bag, *Cyber Law and Cyber Crimes* (Kamal Law House, Kolkata, 2019), pp. 215–225.

seemingly real sexual content using images, video and audio by creating or altering them. Such technologies can have a severe impact on the dignity of children, their privacy and reputation when they are applied against the children. They also cause problems in establishing authenticity of digital evidences and applying the pre-existing legal provisions.¹²

2.8 Distinctive Features of Digital Abuse

Digital abuse implies lack of anonymity, rapidity, persistence and broad geographical coverage. Unlawful material is replicatable and can be re-used even after being initially deleted and offenders can even carry out their web with false identities or across borders. These features present serious hindrances in the way of prevention, investigation and prosecution and reveal the necessity to provide a coherent legal and technological as well as child-focused response.

3. Socio-Legal Impact of Digital Abuse on Children

Digital abuse not only impacts children in the immediate online interaction, but the consequences can be psychological, social, educational and legal. It has a significant effect due to the fact that even after the abusive content or communication is deleted, children might still experience fear, stigmatization and loss of privacy.¹³

3.1 Psychological and Emotional Impact

Sextortion, threats and intimidation, harassment and anxiety, embarrassment and distress are in the online grooming, which may result in anxiety and feelings of fear. Due to the fear of being punished, social stigma, or being exposed to more abuse, children might be reluctant to report abuse. This can enable the offenders to still control the child.¹⁴

3.2 Impact on Privacy and Dignity

Privacy and dignity can be severely impacted by the unauthorized gathering or distribution of photographs, videos or personal data of a child. Even after being removed, digital content can be duplicated and shared again, which leads to the further development of fear of being exposed

¹² Pavan Duggal, *Cyberlaw: The Indian Perspective* (Universal Law Publishing, New Delhi, 2017), pp. 325–330.

¹³ Karnika Seth, *Protection of Children on Internet* (LexisNexis, New Delhi, 2013), pp. 1–15.

¹⁴ National Institute of Public Cooperation and Child Development, *Handbook on Implementation of POCSO Act, 2012*, Ministry of Women and Child Development, Government of India, pp. 15–20.

and repeated victimisation.

3.3 Impact on Education and Family

Depending on online harassment, there could be an impact on focus, attendance at school and peer interactions. Children also do not disclose as there is fear of their parents limiting their access to the internet or even blaming them to have caused the action. Early reporting and recovery depends on a conducive family environment.¹⁵

3.4 Social Stigma and Underreporting

This can lead to bullying of the victims, isolation, and damaged reputation in a social context especially when personal content is shared amongst peers. Underreporting is due to shame, fear, threats and lack of awareness. Secret and child friendly reporting systems are hence necessary.¹⁶

3.5 Impact on Child Rights

Digital abuse can impact on children in their rights to life, dignity, privacy, equality and protection against exploitation. The described approach to children is allowed by Article 15(3) which allows specific provisions regarding children within the protection of life and personal liberty outlined in Article 21 of the Constitution. These principles help in child-centred approach to online protection.¹⁷

3.6 Need for a Socio-Legal Response

Criminalisation is not enough to deal with digital abuse. Digital literacy, parental consciousness, psychological, efficient cyber-investigation, and easy reporting systems must support the provision of legal protection. The usefulness or inefficacy of POCSO can thus be determined by the extent to which it safeguards children and removes subsequent victimisation.

4. Legal Framework Relating to Digital Abuse of Children in India

There is no single law, which deals with all types of digital maltreatment of children in India.

¹⁵ Pavan Duggal, *Cyberlaw: The Indian Perspective* (Universal Law Publishing, New Delhi, 2017), pp. 280–290.

¹⁶ R.K. Bag, *Cyber Law and Cyber Crimes* (Kamal Law House, Kolkata, 2019), pp. 215–225.

¹⁷ Constitution of India, arts. 15(3) and 21; *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

A mix of POCSO, cybercrime, criminal and intermediary regulations and data protection law offer protection.¹⁸

4.1 Protection of Children from Sexual Offences Act, 2012

The main specialised legislation to protect children against sexual assault, sexual harassment and exploitation is the POCSO Act, 2012. Their topicality to digital abuse is especially observed in the provisions related to the electronic communication and pornography.

Section 11 identifies some types of sexual harassment that may be conducted electronically or digitally. Part 13 to 15 covers the use of children to produce pornography and similar possession or storage of such content, which are subject to the latter, by statute. Section 19 institutionalizes an obligatory reporting of offences, especially significant in the digital instances where reporting of offences immediately can help preserve electronic evidence.

Child-friendly procedures that aim to decrease fear, intimidation and secondary victimisation in investigation and trial are also given by POCSO.¹⁹

4.2 Information Technology Act, 2000

Information Technology Act, 2000 is an addition to POCSO in situations which include electronic communication and digital content. Section 67B is also relevant especially in that he, discusses the material that depicts sexually explicit acts or conduct in the form of electronic material involving children.

Therefore, POCSO is more of a protection of children against sexual offence whereas through the Information Technology Act, the electronic and technological aspect of this behaviour is tackled.²⁰

4.3 Information Technology Rules, 2021

The Information Technology (intermediary guidelines and digital media ethics code) Rules, 2021 have due-diligence requirements to bar intermediaries. Their applicability to child

¹⁸ Pavan Duggal, *Cyberlaw: The Indian Perspective* (Universal Law Publishing, New Delhi, 2017), pp. 275–290.

¹⁹ The Protection of Children from Sexual Offences Act, 2012, Sections 11–15 & 19.

²⁰ The Information Technology Act, 2000, Section 67B.

protection incorporates systems to deal with illegal content and accept complaints.

Digital platforms thus play a significant role in establishing harmful content involving children and taking action against it. This process needs to be implemented by establishing effective reporting, clearing away and keeping appropriate information to conduct lawful investigation.²¹

4.4 Bharatiya Nyaya Sanhita, 2023

Whether the Bharatiya Nyaya Sanhita, 2023 covers other behavior related to digital abuse, it can be dependent on the specifics of a case. Perpetrator of digital offences could commit and perpetrate along with sexual offences, deception, intimidation, or cheating amongst others. The BNS thus works with out-of-way child protection laws.²²

4.5 Juvenile Justice Act and Data Protection

The care, protection and rehabilitation of affected children is under the Juvenile Justice (Care and Protection of Children) Act, 2015. Digital Personal Data Protection Act, 2023 is also applicable since children do not only possess the personal data of children that can be misused by criminals but also photographs or other digital records.

4.6 Constitutional Framework

The wider base of child protection is given by the Constitution. Article 21 safeguards life and personal liberty, such as dignity and personal security, whereas Article 14 safeguards equality and Article 15(3) does allow special consideration of children. Articles 39(e) and 39 (f) are another indication of the State obligation towards protection of children against exploitation and ensuring their healthy development.²³

4.7 Integrated Legal Framework

The Indian system is hence decentralized among a number of laws. POCSO offers highly specified safeguarding of sexual crimes, Information technology Act governs electronic crime and all child sexual abuse content, rules on intermediaries act on the obligations of platforms, BNS is used to deal with related criminal activities and the law on data protection safeguards

²¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–4.

²² R.K. Bag, *Cyber Law and Cyber Crimes* (Kamal Law House, Kolkata, 2019), pp. 210–225.

²³ Constitution of India, arts. 14, 15(3), 21, 39(e)–(f); *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

personal data of children.

Nevertheless, the fact that they have such laws does not necessarily guarantee efficient protection. Their performance is reliant on effective execution, management of digital evidence, technology, reporting, the collaboration of law enforcement agencies and digital service. This argues the need to investigate the true effectiveness of POCSO with regard to the new types of digital abuse.²⁴

5. POCSO Act, 2012 and Digital Abuse of Children

The main specialised act to protect children against sexual offence in India is Protection of Children from Sexual Offences Act, 2012. Despite being implemented earlier than the current level of digitalisation, some of the provisions of the Act apply in cases of sexual harassment, exploitation or publication of sexual content of children using technology.

5.1 Section 11 and Online Sexual Harassment

Section 11 specifies what constitutes sexual harassment of a child and clearly enumerates some of the actions that were undertaken using electronic, digital or technological communication means. This is important as sexual harassment online does not mean that it must be physical. Several digital communications, sexual communications or efforts to initiate or maintain inappropriate contact with a child can be covered under the provision in which it has met its statutory requirements.²⁵

5.2 Sections 13–15 and Child Sexual Abuse Material

Section 13- 15 are concerned with the use of children to get involved in pornographic materials and character known to pornographic materials. They apply more specifically to the online realm, where child-related pornography, photos, videos and other specifically sexually-related content can be produced, stored and easily shared.²⁶

A particularly crucial section is 15 since it is through digital devices that abusive material can be stored and re-viewed. Its use can, nonetheless, include inquiries about the purposeful

²⁴ Karnika Seth, *Protection of Children on Internet* (LexisNexis, New Delhi, 2013), pp. 35–55.

²⁵ Justice J.S. Verma Committee, *Report of the Committee on Amendments to Criminal Law* (Government of India, 2013), pp. 384–386.

²⁶ The Protection of Children from Sexual Offences Act, 2012, Sections 13-14.

possession, storage, forwarding, cloud storage and electronic evidence.²⁷

5.3 Mandatory Reporting and Child-Friendly Procedures

Section 19 presents the obligation of reporting the data related to the execution or attempted execution of an offence as stipulated in POCSO. Reporting in the digital cases is urgent due to the risk of losing electronic evidence, as well as the risk of modifying it and abusive content remaining online.

With POCSO also child friendly procedures are offered to reduce fear, embarrassment and secondary victimisation when investigating and trying a case. Such precautions are especially eminent in locations where the child is already a victim of online harassment or disclosure.²⁸

5.4 Digital Evidence and Emerging Challenges

The cases of digital abuse can be based on messages, photos, videos, account information, metadata and device logs. This evidence can be destroyed, obfuscated or sent interjurisdictionally. Several online and anonymous accounts and various digital identities can also make it harder to investigate.

New types of technologies pose more problems, including AI-generated content and deepfakes, since sexually explicit content can be distorted and even completely artificial. Such advances demand specialised skills in cyber-forensic investigations and possibly need additional legal investigation.²⁹

6. Judicial Approach Towards Digital Abuse of Children

The judgment interpretation is relevant when it comes to the application of POCSO and technological abuse in its manifestations that do not even come directly to mind when the law was first amended. Courts have to strike a balance between the protective value of POCSO and concept of criminal justice and reliability of evidence.

²⁷ *Id.* Section 15.

²⁸ *Id.* Section 19.

²⁹ Pavan Duggal, *Cyberlaw: The Indian Perspective* (Universal Law Publishing, New Delhi, 2017), pp. 325–335.

6.1 Just Rights for Children Alliance v. S. Harish

The case of Just Rights for Children Alliance and Anr. v. S. Harish and Ors. declared on 23 September 2024 by the Supreme Court is especially important regarding child sexual abuse material and POCSO Section 15. The Court took into consideration the legal aspects of having and saving such content in electronic devices and failed to adopt a course of action, which would jeopardise the safeguarding effect of the law.

The case is significant in the digital arena as it acknowledges the fact that the procurement and retention of child sexual abuse-related content may be a facilitator to the further exploitation of children. It thus enhances the preventive aspect of POCSO with regards to digitally stored content.³⁰

6.2 Digital Evidence and Child-Centric Interpretation

Electronic evidence like messages, photographs, videos and account details are often relied upon in cases of digital abuse. The validity and trustworthiness of this evidence by the courts should therefore be taken into consideration, especially where the digital contents are subject to manipulation and alteration.

These are also child-centric approach to the judicial approach. Children that are victims of online sexual abuse might already have been humiliated, threatened or their privacy may have been taken away. The judicial processes should therefore reduce the unwarranted disclosure and secondary victimisation without infringement of the right of an accused to a fair trial.³¹

6.3 Emerging Technologies

The inception of AI-generated content, deepfakes, pseudo-anonymous communication, and encrypted communication raises new issues on how judicial interpretation should be. The current laws might cover certain types of such behaviors, yet truly new technological types of abuse might be in need of legal clarification.

Therefore, the convenient use of POCSO can be widened by judicial interpretation, and not unlimited since the latter will never exclude the necessity of any legislative and institutional

³⁰ *Just Rights for Children Alliance & Anr. v. S. Harish & Ors.*, 2024 INSC 716.

³¹ The Bharatiya Sakshya Adhiniyam, 2023, provisions relating to electronic and digital records.

adjustments.³²

7. Efficacy of the POCSO Act, 2012 in Addressing Digital Abuse of Children

Whether POCSO is effective in combating digital abuse does not only rely on the presence of statutory provisions alone but rather on how these provisions are applied to fit the fast-evolving technologically advanced world.

7.1 Strengths of the POCSO Framework

One of the strongest strengths of POCSO is its child-centred approach that is specialised. Section 11 specifically acknowledges some of the technology mediated behaviour and the subsequent Section 13 to 15 gives a guideline to be followed in the use of children to engage in pornography and material related to it. Protective framework will be enhanced further with mandatory reporting under Section 19 and child-friendly procedures.

By establishing the importance of possession and storage of child sexual abuse material, the decision made by the Supreme Court in *Just Rights for Children Alliance v. S. Harish* has given a further read into the argument of what is meant by Section 15, in the digital environment.³³

7.2 Major Limitations

Notwithstanding these advantages, there are various obstacles that have impacts on the effective implementation of POCSO. Digital abuse can be characterized by anonymous offenders, encrypted communication, disappearing messages and cross-border communication. The investigators will have challenges in determining offenders and conservation of electronic evidence.

Another emerging challenge is the AI-generated images and deepfakes. Synthetic content might not involve a real life event, which raises the questions of how the existing provisions are to be implemented, victims and culpable events found.³⁴

³² Pavan Duggal, *Cyberlaw: The Indian Perspective* (Universal Law Publishing, New Delhi, 2017), pp. 325–335.

³³ *Just Rights for Children Alliance & Anr. v. S. Harish & Ors.*, 2024 INSC 716.

³⁴ Pavan Duggal, *Cyberlaw: The Indian Perspective* (Universal Law Publishing, New Delhi, 2017), pp. 280–295.

7.3 Digital Evidence and Institutional Capacity

Successful prosecution entails a specialised set of ability to gather, preserve and confirm electronic evidence. The police and the forensic agencies will, therefore, require proper technological skills. The delay in the process of reporting, loss of digital data and ineffective cooperation between the agencies can undermine investigations.

7.4 Role of Digital Platforms

The digital platforms (social media) are significant in the detection and response of child sexual exploitation. Proper reporting, eradication and maintenance processes have the potential to help in both prevention and investigation. Planning on how to enhance collaboration between platforms and law enforcement agencies is thus needed but with proper consideration of appropriate privacy and due-process measures.

8. Emerging Challenges in Addressing Digital Abuse of Children

The accelerated invention of digital technologies, has brought about new types of abuse that was not perfectly envisaged at the time the laws governing how child protection is practiced were created. Despite the significant legal framework introduced in the POCSO Act, 2012, there are technological, legal, institutional and social challenges of digital abuse.

8.1 Artificial Intelligence and Deepfake Technology

The technology of AI and deep fake can produce realistic synthetic images, videos as well as audio. The misuse they have committed can be a fabricated sexualised material with photographs of a child. This kind of content may result in severe psychological, reputational and privacy-related damages and brings concerns about sufficiency of current legal regulations and the liability of production or dissemination of synthetic material.

8.2 Online Grooming and Sextortion

Online grooming usually starts with seemingly innocent forms of communication in which perpetrators eventually build some trust after which they request personal or intimate content. When criminals risk to reveal such material to get additional pictures, money or compliance, sextortion can occur. Children may be afraid and ashamed to report such offences and therefore

it is important to have confidential and child friendly actions.

8.3 Anonymous Identities and Encrypted Communication

Identifying the perpetrators and gathering the evidence may be challenging when there are several accounts and false identities, as well as encrypted communication. And the data can also be allowed to rest in foreign services or cloud companies, imposing further investigation and jurisdiction issues. Proper investigation should thus be able to strike a balance between child protection and any reasonable interests in privacy.

8.4 Rapid Dissemination and Cross-Border Offences

Information may be duplicated and shared quickly in various locations over the Internet. The copies can still circulate even after the removal of the original material hence further victimisation. There is also the possibility of having offenders, victims and evidence within various countries hence the need to collaborate effectively internationally to combat digital offences.

8.5 Digital Evidence

Photos, emails, videos, system files, details of the account and devices logs can contain good evidence in digital abuse cases. Nevertheless, this evidence might be destroyed, altered, encrypted or manipulated. Deepfakes also make it more difficult to assess authenticity and necessitate specialised cyber-forensic skills.³⁵

8.6 Underreporting and Limited Digital Awareness

Due to fear, shame, stigma, threats or fear of losing access to digital devices, children might be reluctant to report abuse. Inadequate awareness among children, parents and teachers can also make one more vulnerable. Online safety training and an anonymous reporting procedure are thus crucial.

8.7 Institutional and Platform Accountability

These take trained police officers, prosecutors, forensic personnel and judicial officers to be

³⁵ R.K. Bag, *Cyber Law and Cyber Crimes* (Kamal Law House, Kolkata, 2019), pp. 210–225.

enforced. The digital platform is also significant in identifying content that is harmful and can be used to report and collaborate with legitimate investigations. The accountability of platforms should, nonetheless, be available in the context of privacy and the protection of due process.

8.8 Need for Continuous Legal Adaptation

Technology is advancing at a rate higher than the legal provisions. The POCSO framework must thus be regularly review to accommodate AI-generated content, deepfakes, encrypted communication and other threats of misconduct. There should be technological training, institutional coordination, digital literacy and child sensitive support to legal reform.³⁶

9. Suggestions and Legal Reforms

To enhance the effectiveness of POCSO in tackling digital abuse, the measures listed below might be effective:

- a. Regular legal assessment: The current legislation must be assessed to find ways to deal with AI-created sexual material, deepfakes and other types of digital abuse.
- b. Specific digital investigation: Police, prosecutors and forensic staff: Digital evidence, grooming, sextortion, deepfakes and online investigations should be they routinely trained on.
- c. Reporting to be child friendly: There should be a confidential and open system of reporting to help the child report the abuse with no fear of being blamed or punished.
- d. Platform responsibility: Digital platforms ought to enhance mechanisms of detecting, reporting and eliminating content of child sexual exploitation and collaborate with legal investigations.
- e. Digital literacy: Children, and parents/teachers are to be informed on grooming, suspicious communication, privacy, sextortion, and safe reporting.
- f. Cooperation among agencies: There should be enhanced inter-agency cooperation between police, cybercrime agencies, child protection agencies and technology

³⁶ The Protection of Children from Sexual Offences Act, 2012; Karnika Seth, *Protection of Children on Internet* (LexisNexis, New Delhi, 2013), pp. 235–245.

companies, including the method of getting evidence in other jurisdictions.

- g. Child-centred protection: There should be protection of the child dignity, privacy and psychological well-being, and the goal of the protection should be avoiding further victimisation.

10. Conclusion

Digitization of childhood has not only offered new possibilities of communication and education but it has also created new ways, in which child might be abused. Online grooming, sextortion, sexual harassment, child sexual abuse content and AI-generated artificial intelligence or deepfaked content is evidence of ever-increasing digital child abuse.

The POCSO Act, 2012 is an effective thought in the sphere of legal frameworks with its categorisation of electronic means, articulations about sexual exploitation and pornographic content, the compulsory reporting and child-specific methods. Courts have also enhanced its usage to online types of exploitation.

Nevertheless, the statutory requirements are not sufficient to provide a good protection. The anonymity, encryption, cross-border crimes, lack of ability to manage digital evidence and new AI methods pose a big challenge to enforcement. A proper protection follows as needed is legal reform alongside cyber-forensic skills, child friendly reporting, digital literacy, platform responsibility and academic collaboration.

The article concludes that POCSO continues to be a relevant tool that can safeguard children, but its operation in the digital space will rely on its ongoing adaption to the technological transformation. There is a need to have a timely and technologically competent and child focused legal system that considers sustainable protection against the current and the emerging types of digital abuse.