

**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.

Deepfake-Based Sexual Abuse of Children in India: Emerging Challenges under the POCSO Act, 2012

ROBIN BHARTI* AND DR. POOJA**

ABSTRACT

The emergence of AI and deepfake technology has set up new boundaries of sexual abuse and exploitation of children on the Internet. Deepfake can be used to generate and modify or manipulate realistic images, videos and audio including sexually explicit material involving children. This content can be produced without the hunting even being involved, and still greatly harm the privacy, dignity, psychological health and social status of the child. The quick and frequent re-distribution of such content via digital platforms adds to the chances of further victimisation. The Protection of Children against Sexual Offences Act, 2012, is in India the main specialised framework of the protection of children against sexual offences. Its provisions on sexual harassment and the sample on the use of children to obtain pornography have great application on technology-enabled abuse. Nonetheless, the technology of deepfaces implies some serious questions regarding the relevance of current regulations in the scenario in which the content of abuse is created or altered using artificial means. The paper will focus on sexual abuse against children by using deepfakes in India specifically focusing on the POCSO Act of 2012. It examines the applicable law and legal cases and controversies that apply to digital evidence, authoritarianism, reputation of criminals, responsibilities of the platform, and global distribution. It asserts in the study that the current legislation is an essential starting point that demands constant modification in respect to new AI applications. It also finds that proper protection involves a greater clarity of laws, specialised capacity of cyber-forensic, enhanced responsibility of platforms, digital literacy and child-focused redress and inquiry.

Keywords: Deepfake, Artificial Intelligence, Child Sexual Abuse, POCSO Act, Digital Abuse, Cyber Law, Child Protection

I. INTRODUCTION

With the fast evolution of the Artificial Intelligence (AI), machine learning and digital communication, the creation and distribution of digital content has changed. Nevertheless, the technologies have led to new methods of exploitation, especially by children. Deepfake

* Author is a Research Scholar at the Department of Law, Kurukshetra University, Kurukshetra, Haryana, India.

** Author is an Assistant Professor at the Department of Law, Kurukshetra University, Kurukshetra, Haryana, India.

technology is one of the new threats, which is able to both create and manipulate realistic images, videos and audio with the objective to make a person seem to do or to say something that did not actually happen. Its perversion as a sexual tool has raised serious concerns to protect children.¹

Sexual abuse of children with deepfaked technology entails generating, manipulating, or propagating sexually evocative or sexualised digital information, utilizing a child face, identification or photograph. The child can be a passive participant in developing the content, but the content can still seem authentic. The images found on social media or other online platforms can be edited with the help of AI tools and shared via social media, messaging apps, and other online platforms.²

The impacts might not be limited to the creation of the material. Even after removing digital content, it is possible to replicate and download and redistribute it. Children can thus be subjected to further fear, humiliation, anxiety, bullying, loneliness, and reputation damage. Deepfakes can be utilized in blackmail, in sextortion, grooming and online sexual harassment, which contributes to the threat of further exploitation.³

The main specialised laws that protect children against sexually related crimes in India are the Protection of Children against Sexual offences Act, 2012 (POCSO Act). Section 11 acknowledges that some sexual harassment is electronic or electronic in nature and Section 13-15 are concerned with the use of children to access pornography or in other sexual activities. Section 19 gives an option of mandatory reporting. Section 67B of the Information Technology Act, 2000, and the Information Technology Rules, 2021 also play a role in safeguarding children against harmful online content.⁴

Nevertheless, the aspect of abuse carried out with the help of deepfakes poses unique challenges to legal practice as the content is not produced as the result of a real-life sexual act between the child and a partner but could be artificially created. This brings into question the relevance of POCSO provisions, the criminal responsibility, the validity of digital evidence and the identification of culprits. The use of anonymous accounts, cross border platforms with encrypted communication, may also make it even more difficult to investigate.

¹ PAVAN DUGGAL, CYBERLAW: THE INDIAN PERSPECTIVE 325–35 (Universal Law Publishing 2017).

² R.K. BAG, CYBER LAW AND CYBER CRIMES 210–25 (Kamal Law House 2019).

³ PAVAN DUGGAL, CYBER LAW, CYBER CRIME & CYBER SECURITY 245–60 (Universal Law Publishing 2021).

⁴ Protection of Children from Sexual Offences Act, No. 32 of 2012, Sections 11, 13–15, 19, Acts of Parliament, 2012 (India); Information Technology Act, No. 21 of 2000, Section 67B, Acts of Parliament, 2000 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

It is against this backdrop that the current research paper will analyze deep leaked-based sex abuse of children in India with particular reference to the POCSO Act, 2012. It evaluates the form and effects of deepfake abuse, the current legal landscape, legal history and technological challenges, and reviews the necessity of proper legal, institutional, and technological changes that protect children in the digital era.

II. CONCEPT AND NATURE OF DEEPFAKE-BASED SEXUAL ABUSE

A. Meaning of Deepfake Technology

Deepfake technology can be referred to as the ability to use artificial intelligence and machine-learning algorithms to produce or alter audio-visual content in such a way that it seems real. Voice recordings, videos and the pictures of people can be manipulated or created with great realistic quality. Though it has actual uses, the technology taken improperly can be used to facilitate harassment, impersonation, fraud and sexual exploitation.⁵

B. Deepfake-Based Sexual Abuse of Children

Deepfake sexual abuse is an offense carried out with the aid of AI technology to generate, manufacture or distribute sexualized material of a child. The face of the child can be implant to an emphasized image or video that is already structured or new synthetic data can be formed based on publicly available images. The child can not take any part in the creation of the material, but can get severe effects due to its circulation.⁶

C. Forms of Deepfake Abuse

There are various forms of deepfake abuse, such as altered photographs, forged sexual video clips, fake audio, false social-media accounts and content that is digitally altered. Attackers can also dox with the use of deepfakes and threats, online grooming, blackmail or sextortion. The growing availability of AI technologies has lowered the technical challenges to producing manipulated content.⁷

D. Distinctive Features

Deepfake-based abuse is not the same as more traditional forms of digital abuse since the content might look real even though it is fully or partially synthetic. This poses challenges to the victims, parents, investigators and the courts to know who has provided real evidence and

⁵ PAVAN DUGGAL, CYBERLAW: THE INDIAN PERSPECTIVE 325–35 (Universal Law Publishing 2017).

⁶ R.K. BAG, CYBER LAW AND CYBER CRIMES 210–25 (Kamal Law House 2019).

⁷ PAVAN DUGGAL, CYBER LAW, CYBER CRIME & CYBER SECURITY 245–60 (Universal Law Publishing 2021).

who has tampered with evidence. When it goes viral, synthetic content can be shared and re-shared through a variety of sites, which makes it hard to completely eliminate.⁸

III. SOCIO-LEGAL IMPACT OF DEEPFAKE SEXUAL ABUSE ON CHILDREN

A. Psychological and Emotional Impact

Deepfake sexual abuse can result in fear, anxiety, shame, humiliation and emotional distress. When fabricated sexual materials are shared among peers, friends or even family members, a child might become under a lot of psychological pressure. The awareness that the content can occur again and again could create persisting insecurity.

B. Privacy and Dignity

Production and distribution of sexualised material under a child identity is a major encroachment on privacy and dignity. Association of child identity with sexual material can be long-lasting even in a situation where the underlying image is an artificial creation.⁹

C. Social and Educational Consequences

There can be bullying by the victims, and a social and reputational loss. The fear of being exposed can influence the school attendance, the school performance and peer associations. Children could also retreat to social-media sites or other online activities due to the fear of being abused again.¹⁰

D. Family and Social Impact

Children might not report deepfake abuse due to the fear of blame, punishment or limiting or restricting use of digital devices. Parents themselves might not be adequately aware of the technology of deepfaking and might not initially interpret the form of abuse. Families intervention is therefore crucial.

E. Continuing Victimisation

Digital content is easily available and can be downloaded, copied and reproduce continuously. Therefore, the harm might not be fully avoided by misdeletion of the original material. Deepfake technology thus establishes the fact that even with the fact of victimisation, it is possible to perpetrate the crime even after the first time.¹¹

⁸ *Id.* at 260–70.

⁹ INDIA CONST. art. 21; K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

¹⁰ R.K. BAG, CYBER LAW AND CYBER CRIMES 210–25 (Kamal Law House 2019).

¹¹ PAVAN DUGGAL, CYBER LAW, CYBER CRIME & CYBER SECURITY 245–60 (Universal Law Publishing 2021).

IV. LEGAL FRAMEWORK RELATING TO DEEPFAKE-BASED SEXUAL ABUSE IN INDIA

India does not presently have a single comprehensive legislation specifically dealing with deepfake-based sexual abuse of children. The protection is thus based on multiple laws.

A. Protection of Children from Sexual Offences Act, 2012

The POCSO Act offers specific protection of sex crimes against children. Section 11 identifies some types of sexual harassment that are through electronic or digital form. In section 13 to 15, the use of children in consuming pornographic content and other related activities which involve such content have been addressed.

This can be applicable here where deepfaked content has been used to generate or share sexualised materialistic information involving a child. There might be doubts, though, in the areas where the material is purely synthetic and the material does not show a real sexual act with the child.¹²

B. Information Technology Act, 2000

POCSO is supplemented by Information Technology Act that addresses cyber and digital crimes. Section 67B especially applies to electronic content that captures children engaging in erotic sexual activities or behavior. Other clauses related to identity theft, impersonation, cheating or unauthorised access might also be involved depending on the facts.

C. Information Technology Rules, 2021

The Information Technology Rules, 2021 introduce due-diligence norms of intermediaries and introduce an arrangement of unlawful online content. The digital platforms thus play an influential role in responding to complaints, blocking harmful content and collaborating lawful investigations.

D. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 can be used where deepfake abuse includes other criminal behaviors like cheating, criminal intimidation, stalking or other deeds. Its provisions can be enforceable with POCSO and cyber laws.

¹² Protection of Children from Sexual Offences Act, No. 32 of 2012, Sections 11–15, 19, Acts of Parliament, 2012 (India).

E. Bharatiya Sakshya Adhiniyam, 2023

Deepfake cases are very reliant on electronic evidence. Photographs, videos, messages, account information, metadata and device logs can be of investigative and prosecutorial use. Electronic and digital records are to be given the evidentiary framework in the Bharatiya Sakshya Adhiniyam, 2023.

F. Constitutional Protection

Art 14, 15(3) and 21 of the constitution give a significant constitutional basis protection to children. Article 21 safeguards life and personal liberty and got understood and applied to encompass dignity and privacy. Article 15(3) authorizes specific treatment of children, which can help uphold the concept of a protective treatment of new mechanisms of technological misuse.¹³

V. APPLICABILITY OF THE POCSO ACT, 2012**A. Section 11 and Digital Sexual Harassment**

In Section 11, there are some of the forms of sexual harassment that are done electronically or in digital form. In cases where the deepfake content can be sexually harassing, threatening or humiliating a child; the provision can be relevant based on particular facts and statutory provisions.¹⁴

B. Sections 13–15 and Pornographic Material

Mainly important section is in 13 to 15 wherein the deepfake technology is utilized in creation, distribution, transmission, storage or possession of a sexual material involving children. Such material is most likely to be dispensed or victimised repeatedly due to its digital nature.¹⁵

C. Section 15 and Synthetic Material

Section 15 is now specifically important when it comes to digitally archived child sexual abuse content. The ruling of the Supreme Court in *Just Rights for Children Alliance and Anr. v. S. Harish and Ors.* gives a valuable insight on the possessions and storage of such material.

But another issue brought about by deepfake situations is whether the same kind of legal treatment should be given to artificially created material that features a child, as compared to a

¹³ INDIA CONST. arts. 14, 15(3), 21.

¹⁴ Protection of Children from Sexual Offences Act, No. 32 of 2012, Section 11, Acts of Parliament, 2012 (India).

¹⁵ *Id.* Sections 13–15.

material that involves a real child. This problem will have to be interpreted with keen consideration and maybe clarified legally.¹⁶

D. Mandatory Reporting

As stipulated in section 19 of POCSO, information concerning the commission and/or attempted commission of an offence is to be reported. It is especially crucial when dealing with cases of deepfakes when it is necessary to promptly report the audience since the online content can be massively disseminated and the online evidence can be deleted or modified.¹⁷

E. Child-Friendly Procedures

POCSO has child-friendly procedures, which are meant to alleviate fear, intimidations and secondary victimisation. Such precautions are necessary in the deepfake scenarios since children might be undergoing embarrassment, social pressure, and mental distress.

VI. JUDICIAL APPROACH

The interpretation of the judiciary serves a critical role in the implementation of POCSO towards new technological types of child sexual exploitations.

A. Just Rights for Children Alliance v. S. Harish

A notable case when it comes to child sexual abuse material and the section of POCSO is the case Just Rights for Children Alliance and Anr. v. S. Harish and Ors., which was decided by the Supreme Court on 23 September 2024. The Court took into account the legal aspects of the possession and storage of such material and took an approach that reflected the protective nature of legislation.

The decision is especially pertinent to the online realm since child sexual abuse content can be stored and transmitted via electronic devices and the Internet. It underscores the urgent need to deal with the digital content in the ongoing exploitation of children.¹⁸

B. Digital Evidence

Cases of Deepfakes pose a tremendous difficult task of evidence. The courts might be required to rule on whether an image, video or audio recording is authentic, distorted or completely artificial. Technical analysis, metadata analysis, and device logs and technologies could thus be necessary.

¹⁶ Just Rights for Children Alliance & Anr. v. S. Harish & Ors., 2024 INSC 716 (India).

¹⁷ Protection of Children from Sexual Offences Act, No. 32 of 2012, § 19, Acts of Parliament, 2012 (India).

¹⁸ Just Rights for Children Alliance & Anr. v. S. Harish & Ors., 2024 INSC 716 (India).

C. Need for Judicial Caution

Courts should secure children against further victimisation as well as grant them right to fair trials. The availability of the deepfake technology puts the role of the judiciary in assessing authenticity as especially significant since seemingly authentic content can be manufactured artificially.

VII. EMERGING CHALLENGES

A. AI-Generated Sexual Content

With minimal technical skills and the assistance of AI tools, it is possible to produce highly realistic sexualised content in the form of images and videos. The increasing accessibility of such tools may increase the scale of deepfake abuse.

B. Identification of Victims and Offenders

A criminal can use the pictures acquired in one of the public profiles without the consent of the child. False statements and anonymity may render identification challenging.¹⁹

C. Digital Evidence and Authenticity

The conventional approaches to studying the digital content can be not necessarily enough to detect the advanced manipulation. It has to be done with specialised forensic tools and trained investigators.

D. Rapid Dissemination

Deepfake content can be shared on various platforms in a relatively short amount of time. The copies may still be left in other places even when the original content has been taken.

E. Cross-Border Challenges

Criminals, victims, digital evidence, and sites can be in various jurisdictions. Seeking information of foreign service providers can slow down investigation and prosecution.

F. Platform Accountability

The social-media and other intermediaries play a significant role in identification, reporting, stifling of the destructive contents. Proper collaboration with law-enforcement agencies should be the rule in affording privacy and due-process protections.

¹⁹ PAVAN DUGGAL, CYBERLAW: THE INDIAN PERSPECTIVE 325–35 (Universal Law Publishing 2017).

G. Underreporting

Children would be reluctant to report about deepfake abuse due to the shame, fear of being socially punished, or fear that reporting such abuse will advance further sharing of tapes. It is therefore imperative to have child-friendly and confidential reporting systems.

VIII. EFFICACY OF THE POCSO ACT, 2012

POCSO offers a legitimate basis on child sexual exploitation protection. Its awareness of sexual harassment through technology and its clauses on pornographic content render it pertinent to online harassment.

But the Act did not target in particular the advanced AI generated content now accessible using deepfake technology. The difference between the real and synthetic material raises ambiguity on the extent of the current provisions. Moreover, POCSO is not sufficient to cover all the issues of deepfake abuse since other branches of law, such as digital platforms, electronic evidence, data protection and cyber-forensic investigation, are involved.

The practicality of POCSO is thus contingent on the alignment with the laws of cybercrime, the statute of digital evidence, re-intermediary regulation and technology savvy. The protection provided by the law should also be followed by effective enforcement.

IX. SUGGESTIONS AND LEGAL REFORMS

Child protection in India needs to take a technology-sensitive and all-encompassing approach due to the rise of deepfake-based sexual abuse. Despite the comprehensive legal protection, especially the POCSO Act, 2012, there are cases where technological innovations pose scenarios that may need more explicit legal protections, institutional readiness, and proactive devices.

To start with, AI-generated sexual abuse needs to be clearly recognized by legislation. There should be clear laws that regulate the production, editing, possession, printing and distribution of sexually explicit deepfake information that involves children. The law ought also to demarcate the area where the contents are entirely synthetic yet the identities, face or personal photographs of a recognizable kid are utilized. Such elucidation would lessen confusion on investigation and prosecution.

Second, there should be a periodic review and enhancement of POCSO framework. Due to the dynamic pace of technology, statutory provisions must be in a position to deal with new modes of technology-sustained sexual abuse. Precise instructions can be created on how to apply

Sections 11 and 13-15 to AI-generated and manipulated content. The protective nature of POCSO must be the foremost priority whilst not violating tenets of legality and fair-trial.

Third, cyber-forensic infrastructure needs to be enhanced across the country. Deepfakes involve the application of the technical expertise necessary to tell whether photographs, videos or audio recordings have been altered. Regular training of police officers, forensic experts, prosecutors and judicial officers in AI technologies, deepfake detection, metadata analysis, electronic evidence preservation and digital tracing should be provided.

Fourth, technologies of quick preservation of digital evidence must be created. Deepfake content is easily removable, movable or editably between platforms and within a brief amount of time. Relevant procedures in obtaining relevant devices, account information, metadata and online records whilst meeting any legal safeguards should therefore be in place in investigating agencies. Effective preservation is a great way to enhance the credibility of prosecution.

Fifth, more responsibility needs to be on digital media. Social-media platforms, messaging service, and other ad hoc intermediaries ought to have an easily contactable method of reporting suspected child sexual abuse content and AI-generated sexual content. They ought to devise useful detection and eradication mechanisms and collaborate with legitimate investigations. Concurrently, section 15 of the status offences law ought to add mechanisms to handle any form of unjustified removals and protection of bona fide privacy rights.

Sixth, digital literacy and preventive education should be strengthened. The children are to be informed of the danger of posting photos, accepting strangers, responding to suspicious messages and engaging with strangers. The parents and teachers are also to be trained in order to spot the indicators of being exploited online. The awareness programmes need to provide information that victims are not responsible of a manipulated or fabricated content.

Seventh, reporting mechanisms should be increased with confidential and kid friendly reporting mechanisms. Because of shame, fear of punishment or fear that the content will further spread, children might be reluctant to report deepfake abuse. Reporting systems must thus be open, confidential and sensitive to age and circumstances of the child. Removal of harmful material as well as preservation of evidence should be assisted as soon as possible.

Eighth, legal response should include psychological and social assistance. Even when it is the fabricated content, deepfake sexual abuse can result in humiliation, anxiety, fear and social isolation. Counselling, family support together with proper rehabilitation services should therefore be offered to victims in need. Prosecution should merely be an objective but recovery and the safeguarding against recurring victimisation should also be part of the objective.

Ninth, there is a need of the improved inter-agency coordination. This can be done through effective investigation with police officers, cybercrime centers, forensic centers, child-safety authorities and online platforms. Orchestrated protocols have the potential to decrease delays and enhance evidence preservation and analysis. International platforms or international offenders should also be enhanced in terms of cooperation.

Tenth, there should be improved cooperation with the international cooperation. Deepfake-enabled abuse may be an intra-jurisdiction issue, or weaken the jurisdiction of the server and platform, as well as the perpetrators and victims in various jurisdictions. There is a need to have effective processes of receiving electronic evidence of foreign service providers as well as investigating transnational crimes. The jurisdictional barriers that child-protection activity can experience can be avoided with the cooperation of various countries.

Eleventh, there are AI tools that are able to produce sexualised content that should receive special attention. Access control should be embraced by the developers and service providers to avoid their systems to be abused and produce sexual content generated on children. Legal regulation can be supplemented by technical solutions, including detection systems, and damaging prompt and reporting systems.

Lastly, reforms of law must strike a balance between basic rights and child protection. The control of deepfake technology must safeguard children against sexual exploitation but must uphold privacy, freedom of speech, due process and other constitutional rights. The long-term vision is to establish a legal system which responds to technological advances, and ensures that the law is able to keep up with technological development when it comes to protecting children. An integrated set of POCSO reform, cyber-forensic potential, platform responsibility, digital literacy, kid-friendly reporting and institutional collaboration is hence crucial in successfully addressing deepfake-driven sexual mistreatment in India.

X. CONCLUSION

In India, a novel type of digital child exploitation that is highly severe and fast growing is deepfake-based sexual abuse. Artificial Intelligence has the potential to cause significant harm even when a child did not create content by creating realistic sexualised images, videos and other content using their face or identity. This kind of abuse impacts the privacy rights, dignity and psychological well-being and social reputation of the child. The damage can persist even after the original material is taken down as any digital content can be reproduced and further shared.

The POCSO Act of 2012 has a significant legal aspect on ensuring that children are not exploited sexually. Its sexual harassment provisions, electronic communication and pornographic material can be brought into play to cope with various forms of abuse that have the technology as an enabler. But the deepfake technology poses fresh legal challenges, especially when the content is not produced organically but rather artificially and is not a portrayal of a real sexual act involving the child. Issues with criminal liability, the extent of current stipulations, control over synthetic material and its distribution, and the integrity of electronic evidence should be given attention.

The current legal system should somehow be supplemented with the other laws addressing the cyber offences, electronic evidence and intermediary responsibility. The judicial interpretation may help to use the current provisions to the emerging technological cases, but the courts may not be able to handle all the emerging types of AI-based abuse. To keep child-protection laws up to date, as technology evolves, they should be periodically reviewed by legislation.

Specialised cyber-forensic capabilities and trained investigators with the ability to detect manipulated content and track culprits are also needed to effectively protect. Platforms should also be able to report effectively and have a removal system in place and work in collaboration with legal investigations. Concurrently, children, parents and teachers should receive the necessary education related to the digital-safety so that the risks could be detected in the initial phase.

Lastly, sexual abuse in the event of deepfakes needs to be child-centred. In order to recover the affected children, confidential reporting, psychological support and protection against any further exposure is important. A synchronized efforts of POCSO, cyber law, technological benefits, accountability of platforms, and digital consciousness and organizational collaboration are thus required. This type of strategy can enhance the ability of India to safeguard children against the new types of AI-enabled sexual exploitation and make sure that the law does not lag behind technological advancements.
