IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CHILD PROTECTION IN THE AGE OF GENERATIVE AI: RETHINKING POCSO AND INTERMEDIARY LIABILITY IN INDIA

Dr. Sheena Thomas[1], Dr. Bharati G Ganawari [2]

[1]Associate Professor of Law, [2]Associate Professor of Law,

Government Law College Holenarasipura, Under the Department of Collegiate Education,Bengaluru,

Government Law College, Holenarasipura, Hassan District, Karnataka State, India, 573211

Abstract: The rapid transformation of the digital environment has changed not only how children communicate and participate online, but also how child sexual exploitation and abuse material (CSEAM) can be created, stored, shared and repeatedly circulated. Social-media platforms, messaging services, cloud infrastructure and, more recently, generative artificial intelligence have created digital spaces in which harmful material can travel across borders within seconds and remain accessible long after the original abuse has occurred. The continuing circulation of such material can therefore prolong the violation of a child's dignity, privacy and personal security. These developments raise an increasingly difficult legal question as to what extent should online platforms be held responsible for unlawful material that they did not themselves create but that is transmitted or hosted through their services?

This question has gained particular significance in India following the Supreme Court's decision in Just Rights for Children Alliance & Anr. v. S. Harish & Ors., 2024 INSC 716, which adopted a broader understanding of digital possession in the context of child sexual-abuse material under the Protection of Children from Sexual Offences Act, 2012 (POCSO). The Court's reasoning demonstrated the need to interpret child-protection law in light of contemporary digital realities. The issue has now moved towards a more complex institutional question. In 2026, the Supreme Court agreed to examine a plea concerning the possible prosecution of online platforms under POCSO in cases involving the hosting of, or failure to report, child sexual-abuse material. Although the proceedings remain pending and do not establish criminal liability against intermediaries, they bring into sharper focus the relationship between POCSO's reporting obligations and the conditional safe-harbour protection available under the Information Technology Act, 2000. Generative artificial intelligence further complicates this legal landscape. AI-generated images, manipulated photographs, synthetic videos and other forms of digitally fabricated sexual material involving children challenge conventional understandings of creation, possession and dissemination. This article examines these developments through the broader framework of intermediary liability, platform governance and digital constitutionalism. It argues that Indian law should move beyond the rigid choice between intermediary immunity and automatic platform liability and instead adopt a proportionate, capability-based model of responsibility. Under this approach, platform responsibility would be assessed in light of knowledge, technological capability, and degree of control, foreseeable risk and compliance with statutory duties. Such a framework can strengthen child protection while preserving the constitutional values of privacy, freedom of expression, due process and responsible technological innovation.

Index Terms - POCSO, intermediary liability, child sexual abuse material, CSEAM, artificial intelligence, generative AI, platform governance, safe harbor, digital constitutionalism, India.

I. INTRODUCTION

The internet has transformed the way children communicate, learn and participate in social life. At the same time, it has created new environments in which children can be sexually exploited and in which abusive material can circulate long after the original act has taken place. What once required physical possession of photographs, videos or other forms of recorded material can now occur through digital systems capable of storing, reproducing and transmitting information almost instantaneously? The resulting problem is therefore not simply one of individual criminal behavior. It is increasingly a problem of digital infrastructure and institutional responsibility.

Child sexual exploitation and abuse material occupies a particularly difficult position within this environment. Once such material enters a digital ecosystem, it can be copied and redistributed repeatedly, creating continuing harm to the child depicted. A victim may therefore experience repeated violations of privacy and dignity even after the original abuse has ceased. The technological capacity of platforms to facilitate this circulation has consequently become relevant to the broader question of legal responsibility.

The Indian legal system is now confronting this problem at an important moment. The Supreme Court's decision in Just Rights for Children Alliance & Another v. S. Harish & Ors., 2024 INSC 716, marked a significant development in the interpretation of digital possession and child sexual-abuse material under POCSO. The Court rejected the proposition that online viewing could automatically be separated from possession or control and restored criminal proceedings that had been quashed by the Madras High Court. The judgment demonstrated that concepts developed in an earlier technological environment must sometimes be interpreted in a manner responsive to the realities of digital conduct.

The next question is considerably more difficult. If an individual can incur legal responsibility through possession or control of abusive digital material, what should be the position of the platform through which the material is stored, transmitted, recommended or accessed? Does the platform's status as an intermediary provide sufficient protection from liability? Or can statutory duties under POCSO operate independently of the intermediary's protection under Section 79 of the Information Technology Act, 2000?

This question has acquired contemporary relevance following the Supreme Court's decision in 2026 to examine a plea seeking prosecution of online platforms under POCSO in relation to child sexual-abuse material and alleged failures to report such content. The Court has issued notice to the Union government, including the Ministry of Electronics and Information Technology and the Ministry of Law and Justice, and the concerned intermediaries are being brought into the proceedings. The matter remains pending and should therefore be approached with doctrinal caution. Nevertheless, the proceedings provide an important opportunity to reconsider the relationship between intermediary status, statutory duties and technological capability.

The central argument of this article is that Indian law should avoid both extremes. Treating platforms as automatically criminally responsible for every unlawful item uploaded by users would undermine the rationale of intermediary protection and could encourage excessive monitoring and censorship. At the other extreme, treating intermediary status as an almost complete shield against responsibility would fail to account for the technological and institutional power exercised by contemporary platforms.

A more convincing approach is to develop a proportionate, capability-based model of platform responsibility. Under this model, legal responsibility should become stronger when a platform has actual knowledge of unlawful material, possesses meaningful technological capacity to detect or prevent its circulation, exercises significant control over its dissemination, and nevertheless fails to comply with clearly established legal duties. The objective should not be to transform every intermediary into a publisher, but to recognize that technological power can generate corresponding legal responsibilities.

II. RESEARCH METHODOLOGY AND SCOPE

This study follows a **doctrinal and comparative legal research approach** to examine the emerging question of intermediary responsibility for child sexual-abuse material in India's digital environment. The doctrinal analysis is primarily based on the existing legal framework governing child protection and online platforms, particularly the **Protection of Children from Sexual Offences Act, 2012 (POCSO), the Information Technology Act, 2000,** and the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.** Particular attention is given to Sections 15, 19, 21 and 30 of POCSO, along with Sections 67B and 79 of the Information Technology Act, as these provisions provide an important foundation for understanding the relationship between child-protection obligations and intermediary safe-harbour protection.

The study also examines the developing judicial approach of the Supreme Court of India, with particular focus on Just Rights for Children Alliance v. S. Harish. The judgment is significant because it demonstrates how concepts such as possession and control may need to be understood differently when the underlying conduct takes place in a digital environment. The article also considers the Supreme Court's emerging proceedings in 2026 concerning the possible liability of online platforms under POCSO. Since the matter is still pending, the discussion does not treat the Court's decision to examine the issue as an indication of the final outcome. Instead, the proceedings are used to identify and analyse the larger constitutional and statutory questions that the Court may ultimately be required to address.

A comparative perspective is included to place India's developing approach within the wider international debate on platform responsibility. The **United Kingdom's Online Safety Act** is considered particularly relevant because it reflects a broader movement away from relying solely on the removal of unlawful content after it has been reported. Its emphasis on risk assessment, preventive measures and systemic platform responsibility provides a useful point of comparison for considering possible directions in Indian law. The comparison, however, is not intended to suggest that the UK model can simply be transplanted into the Indian legal system. Rather, it helps identify principles that may inform India's own constitutional and regulatory framework.

Finally, the study considers the growing influence of **generative artificial intelligence** on the production and circulation of child sexual-abuse material. AI-generated images, manipulated photographs and synthetic videos challenge traditional assumptions about what constitutes original, authentic or digitally possessed material. The article therefore explores whether existing intermediary-liability principles are sufficiently equipped to deal with these emerging forms of abuse, or whether the increasing technological capabilities of platforms require a clearer and more carefully balanced framework of responsibility. The broader aim is to examine how Indian law can strengthen child protection while continuing to respect privacy, due process, freedom of expression and responsible technological innovation.

III. THE DIGITAL CHILD-PROTECTION PROBLEM

The legal treatment of child sexual-abuse material has traditionally focused on the person who creates, possesses or distributes it. Digital technologies complicate this framework because several different actors can now participate in the lifecycle of abusive material without necessarily being involved in the original act of exploitation. A photograph may be created by one person, uploaded by another, stored on a cloud server, redistributed through a messaging service, indexed by a search engine and recommended through an algorithm. The original act and the subsequent digital circulation may therefore involve entirely different actors.

This technological fragmentation creates a corresponding fragmentation of legal responsibility. Criminal law can identify the person who intentionally creates or distributes abusive material relatively clearly. It is more difficult to determine the responsibility of a platform that does not create the material but possesses the technical ability to detect and remove it. The difficulty becomes even greater where the platform receives a report, detects repeated uploads through automated systems or becomes aware of systematic abuse occurring through its services.

The persistence of CSEAM makes this problem especially serious. The harm suffered by a child does not necessarily end when the material is removed from its original source. Copies may continue to exist elsewhere, and each subsequent circulation may expose the victim to another violation of privacy and dignity. The digital environment therefore changes the temporal character of child sexual exploitation. Harm becomes potentially continuous rather than confined to the moment of the original offence.

The United Nations Committee on the Rights of the Child has recognized that children's rights must be protected within the digital environment, including in relation to artificial intelligence, algorithms, automated systems and data processing. General Comment No. 25 emphasizes that digital technologies can create both opportunities and risks for children and that States have responsibilities to ensure that children's rights remain protected in technologically mediated environments.

The implications for Indian law are substantial. A legal framework concerned exclusively with the identity of the original uploading may fail to address the institutional structures that allow abusive material to remain available, searchable or repeatedly distributable. This does not mean that platforms should automatically become criminally liable. It means that intermediary law must increasingly consider the platform's own conduct and capabilities.

IV. POCSO IN THE DIGITAL ENVIRONMENT

The Protection of Children from Sexual Offences Act was enacted in 2012 as a comprehensive statute designed to protect children from sexual assault, sexual harassment and exploitation. Although the Act was not drafted specifically for the era of generative artificial intelligence, its provisions are sufficiently broad to intersect with several forms of digitally mediated abuse.

Section 13 addresses the use of children for pornographic purposes, while Section 15 deals with the storage of pornographic material involving a child. Section 19 creates a reporting obligation, and Section 21 establishes consequences for failure to report or record a case. These provisions demonstrate that POCSO is not concerned exclusively with the original act of abuse. It also seeks to interrupt the conditions through which exploitation can continue.

The significance of Section 15 has increased considerably in the digital context. Physical concepts of possession do not always correspond neatly with digital practices. A person may access material without downloading it, maintain control over material stored remotely or repeatedly access content through a digital service. Consequently, courts have increasingly been required to interpret concepts such as possession and control in light of the realities of digital technology.

Section 67B of the Information Technology Act reinforces this framework by criminalizing various forms of electronic material involving children in sexually explicit or abusive contexts. POCSO and the Information Technology Act therefore operate within an overlapping legal environment in which child protection and digital regulation intersect.

The difficult question is how these statutory obligations interact with intermediary safe harbour. A platform may not be the author of the material, but the platform may nevertheless have separate legal obligations once it becomes aware of the material. The distinction between authorship and responsibility is therefore central to the emerging debate.

V. JUST RIGHTS FOR CHILDREN ALLIANCE V. S. HARISH: CONCEPTUALIZING DIGITAL POSSESSION

The Supreme Court's judgment in Just Rights for Children Alliance & Another. v. S. Harish & Others., 2024 INSC 716, represents a significant turning point in Indian jurisprudence concerning child sexual-abuse material. The case arose from proceedings involving the possession and viewing of material depicting child sexual exploitation. The Madras High Court had adopted an interpretation under which mere viewing of such material without downloading it did not necessarily constitute possession under Section 15 of POCSO. The Supreme Court rejected this narrow approach and restored the criminal proceedings.

The importance of the judgment extends beyond the particular facts of the case. It demonstrates that legal concepts developed around physical objects cannot simply be transplanted into a digital environment without considering how control operates in cyberspace. Digital possession can be conceptually different from physical possession. A user may exercise control over material without possessing a physical copy in the conventional sense. The ability to access, retain, manipulate or repeatedly view digital material may demonstrate a form of control that has legal significance.

This reasoning is important for the intermediary-liability debate, but it must be approached carefully. The Supreme Court's judgment concerned the conduct of individuals rather than establishing a general principle that platforms possess every piece of material passing through their systems. The legal relationship between an individual user's possession and a platform's technological control cannot simply be assumed.

Nevertheless, the decision opens an important conceptual door. If digital control is capable of carrying legal significance, courts may increasingly have to examine the nature and degree of control exercised by technological intermediaries. Contemporary platforms are not merely passive channels. They determine visibility, organize information, recommend content, operate moderation systems and possess substantial technical control over the architecture through which information circulates. The central issue is therefore not whether platform control is identical to individual possession. It is whether such control should influence the determination of independent statutory responsibilities.

VI. SECTION 19 OF POCSO AND THE QUESTION OF KNOWLEDGE

One of the strongest legal foundations for platform responsibility may lie not in the concept of possession but in the reporting obligations imposed by Section 19 of POCSO. This section reflects a legislative decision that child sexual offences require proactive reporting. The obligation is designed to prevent situations in which persons who become aware of abuse remain passive observers. Section 21 reinforces this approach by providing consequences for failure to report.

The application of this framework to digital platforms raises a difficult issue concerning knowledge. A platform may initially have no knowledge that unlawful material exists. It may therefore be difficult to justify criminal liability merely because a user uploads prohibited content. However, the legal position may change once the platform receives credible information concerning the material. Consider a platform that receives a specific complaint identifying material depicting child sexual exploitation. If the platform confirms the complaint, removes the material and reports the matter in accordance with applicable law, the platform's conduct is fundamentally different from that of a platform that receives repeated reports and fails to respond. The same distinction becomes even more significant where the platform's own technological systems identify potentially abusive material.

If a platform voluntarily deploys automated systems capable of identifying known CSEAM, the question arises whether the output of those systems can contribute to the determination of institutional knowledge. It would be conceptually difficult to argue that a platform has no knowledge whatsoever of a category of material that its own systems repeatedly identify and escalate internally.

At the same time, technological detection should not automatically be equated with legal certainty. AI systems can produce false positives and may misclassify lawful material. The existence of an algorithmic flag should therefore trigger appropriate human and legal review rather than automatically establish criminal culpability. The appropriate legal inquiry should consequently focus upon what the platform knew, what it reasonably should have known, what it was capable of knowing and what it did after acquiring relevant information.

VII. SAFE HARBOR AND ITS LIMITS

Section 79 of the Information Technology Act occupies a central position in the intermediary-liability framework. Safe harbor serves an important function because modern platforms cannot realistically inspect every piece of user-generated information before it becomes available online. Without some form of protection, the scale of contemporary digital communication could make intermediary operation legally unsustainable.

However, safe harbor is conditional rather than absolute. Its purpose is not to eliminate every form of platform responsibility but to prevent intermediaries from being automatically treated as publishers or originators of user-generated content. This distinction becomes particularly important in the context of POCSO. A platform may retain its status as an intermediary while simultaneously being subject to statutory duties concerning unlawful content. The fact that a platform did not create the material does not necessarily answer whether it complied with a separate obligation imposed by law.

The IT Rules reinforce this understanding by establishing due-diligence obligations and contemplating technological measures concerning child sexual-abuse material. The framework also recognizes the importance of human oversight, accuracy, fairness and privacy when automated tools are deployed. The emerging legal question is therefore not whether safe harbor should exist. It should. The more difficult question is what conduct should cause a platform to lose or limit the protection that safe harbor provides. A balanced approach would avoid treating the mere presence of unlawful content as sufficient. Instead, courts should examine the platform's knowledge, conduct, technological capability and compliance with clearly defined statutory obligations.

VIII. GENERATIVE AI AND THE EMERGENCE OF SYNTHETIC CSEAM

Generative artificial intelligence creates a new dimension in the child-protection debate because it challenges assumptions about how abusive material is produced. Traditional CSEAM generally involves the recording or depiction of an actual child. Generative technologies can create synthetic images or videos without requiring the same form of physical recording. Existing photographs can also be manipulated through face-swapping or other synthetic-media techniques. Where a real child's identity is incorporated into synthetic sexual material, the victim may suffer reputational, psychological and dignitary harm even if the underlying image is artificial. The problem is further complicated when the material does not correspond to a real identifiable child. The legal system must then determine whether and how synthetic representations of children should be treated under existing criminal law.

India's 2026 amendments to the Information Technology Rules are particularly relevant because they address synthetically generated information and include material containing child sexual exploitative and abuse material within the regulatory framework. This indicates an important shift in Indian technology regulation. The legal system is beginning to recognize that AI-generated content may require distinct governance mechanisms rather than being treated simply as another category of user-generated information.

However, regulation cannot stop at defining prohibited synthetic content. It must also address the systems through which such content is generated and disseminated. If an AI platform provides a service capable of generating abusive synthetic material, questions arise concerning the platform's design choices, safety measures, detection systems and response mechanisms. These questions are fundamentally questions of AI governance. The future legal framework will therefore need to consider not merely what content was produced, but also what technological architecture made the production possible.

IX. AI MODERATION AND HUMAN RESPONSIBILITY

Artificial intelligence has considerable potential to strengthen the protection of children in the digital environment. Given the enormous volume of content generated and shared through contemporary online platforms, human moderators alone cannot realistically identify every instance of child sexual-abuse material. Automated systems can assist by detecting known abusive material through digital fingerprints or hashes, identifying patterns of repeated uploads and drawing attention to content that may require

urgent human review. In this sense, AI can significantly improve the speed and scale of content moderation. At the same time, however, the increasing reliance on automated systems raises important legal and ethical concerns. An AI system does not interpret law in the same way as a court or a trained legal decision-maker. It works through statistical patterns, training data and programmed or learned classifications and may identify content as potentially harmful without being capable of determining whether all the legal elements of a criminal offence are actually satisfied. This distinction becomes particularly important where automated decisions may lead to the removal of content, suspension of accounts, reporting to law-enforcement authorities or other consequences with serious legal implications. AI should therefore function as a **tool for detection and assistance rather than a substitute for human legal judgment**. Meaningful human oversight should form an essential part of any high-risk content-moderation system, with platforms being able to demonstrate how flagged material is reviewed, what standards guide those decisions, how mistakes are identified and corrected, and how significant decisions are recorded. Independent auditing of such systems should also be encouraged to assess their accuracy, false-positive and false-negative rates, potential bias, data-governance practices and compliance with procedural safeguards. The objective should ultimately be to use technological capability to strengthen child protection without allowing automated systems to become an opaque form of digital punishment.

X. PRIVACY, ENCRYPTION AND DIGITAL CONSTITUTIONALISM

The demand for stronger platform responsibility must be balanced against constitutional rights. Digital platforms process enormous quantities of personal information. Measures designed to detect child sexual-abuse material may involve analyzing images, communications, metadata or behavioral patterns. Such measures can therefore have significant implications for privacy. The problem becomes particularly acute in relation to encrypted communication. End-to-end encryption is designed precisely to prevent intermediaries from accessing the contents of communications. If platforms are required to proactively detect unlawful material within encrypted communications, the legal system may create pressure for technical mechanisms that weaken or circumvent encryption.

The issue should not be reduced to a conflict between privacy and child protection. Both interests have constitutional and social importance. The more appropriate approach is proportionality. Any intrusive detection mechanism should have a clear legal basis, pursue a legitimate objective, be necessary for that objective and remain proportionate to the rights affected. It should also incorporate procedural safeguards, data minimization and independent oversight.

The constitutional question is therefore not whether the State may protect children online. Clearly, it must. The question is how that protection can be achieved without creating architecture of indiscriminate surveillance. This is where digital constitutionalism becomes particularly important. Constitutional principles must continue to operate even when rights are exercised through privately controlled technological infrastructure.

XI. COMPARATIVE PERSPECTIVES

The international regulatory landscape demonstrates that intermediary regulation is increasingly moving away from a purely reactive model. The United Kingdom's Online Safety Act provides a useful example. Its regulatory framework requires in-scope services to conduct children's risk assessments and implement appropriate measures where children are likely to access the service. The framework also contains duties concerning illegal content and child sexual exploitation and abuse. The significance of this approach lies in its focus on systemic risk rather than isolated pieces of content. Instead of asking only whether a platform has removed a particular unlawful item after receiving a complaint, the regulatory framework asks whether the platform has designed and operated its service in a manner that adequately manages foreseeable risks.

This approach offers an important lesson for India. The Indian framework already contains elements of proactive regulation, and the 2026 amendments concerning synthetically generated information demonstrate a willingness to regulate emerging technological risks. India could build upon these foundations without simply reproducing foreign legislation. A particularly useful principle would be to require high-risk platforms to assess foreseeable child-safety risks associated with their technological

architecture before harm occurs. Such a model would shift the emphasis from reactive content moderation to preventive platform governance.

XII. A CAPABILITY-BASED MODEL OF PLATFORM RESPONSIBILITY

The central proposition of this article is that intermediary responsibility should be connected to capability rather than determined exclusively by formal classification. The first level should protect genuinely neutral intermediaries. Where a platform has no knowledge of unlawful material, has received no credible notice and has no reasonable basis to identify the material, strong safe-harbor protection remains justified.

The second level begins when a platform receives credible information concerning potentially unlawful CSEAM. At that point, the platform should have clearly defined obligations to assess the material, restrict further dissemination where appropriate, preserve relevant evidence and comply with applicable reporting duties.

The third level arises when the platform encounters repeated or systemic instances of the same material, account or network. Repeated occurrence can transform an isolated incident into a foreseeable platform risk. In such circumstances, the platform should be expected to consider measures designed to prevent recurrence rather than repeatedly removing individual copies.

The fourth level concerns technological capability. A platform that possesses reliable technology capable of identifying known categories of CSEAM occupies a different legal position from a platform that genuinely lacks such capability. The law should nevertheless distinguish technological possibility from technological reliability. A detection system that produces large numbers of false positives cannot simply become the basis for automatic criminal liability.

The fifth and strongest level concerns institutional failure. Where a platform possesses actual knowledge, substantial technological capability, meaningful control and established legal duties, yet deliberately or recklessly fails to respond, the case for serious regulatory or criminal consequences becomes significantly stronger. This model does not eliminate safe harbor. Instead, it makes safe harbor compatible with responsible digital governance.

XIII. CRIMINAL LIABILITY MUST REMAIN DISTINCT FROM REGULATORY FAILURE

As India considers expanding the responsibilities of online platforms in relation to child sexual-abuse material, it is equally important to ensure that stronger regulatory obligations do not gradually develop into a form of **strict criminal liability.** The mere presence of unlawful content on a platform should not, by itself, be sufficient to establish criminal responsibility on the part of the platform or its officers. Holding platforms criminally responsible for every failure of detection could therefore create an unrealistic standard of liability and may undermine the very rationale behind intermediary safe-harbor protection.

Criminal liability should instead be based on clearly defined statutory requirements and an appropriate level of culpability. Courts should carefully distinguish between an **unavoidable technological failure** and conduct that reflects deliberate, reckless or conscious disregard of a known legal obligation. A platform that makes genuine efforts to comply with the law, adopts reasonable detection mechanisms and responds appropriately when potential CSEAM is identified should not automatically be placed in the same legal category as a platform that knowingly ignores credible complaints, repeatedly fails to act despite clear warnings, or deliberately disables effective safety mechanisms. The circumstances surrounding the platform's conduct, including what it knew, what it was reasonably capable of doing and how it responded to the situation, should therefore form part of the legal assessment.

This distinction becomes even more important where artificial intelligence is used for content moderation. Automated detection systems inevitably have limitations and may generate both false positives and false negatives. A platform that deploys a good-faith moderation system, subjects flagged material to appropriate human review, removes confirmed CSEAM and makes the necessary reports should not be treated as though it intentionally facilitated the unlawful material merely because its technology failed to

identify every instance. Conversely, where a platform repeatedly receives credible reports, possesses the technological means to respond, understands the seriousness of the material and nevertheless chooses not to act, the circumstances may justify a significantly stronger regulatory or criminal response.

The emerging framework should therefore maintain a clear distinction between **regulatory responsibility and criminal culpability**. Regulatory law may reasonably impose preventive duties, reporting requirements, auditing obligations and risk-management responsibilities upon platforms. Criminal law, however, should remain concerned with conduct that satisfies the specific statutory elements of an offence and the required degree of culpability. Maintaining this distinction will allow India to strengthen child protection and platform accountability without creating an unnecessarily broad or uncertain system of criminal liability. In the long term, such an approach would also provide greater legal certainty for courts, regulators and technology companies while preserving the fundamental principles of fairness and due process within India's intermediary-liability framework.

XIV. REFORMING THE INDIAN FRAMEWORK

The emerging debate on intermediary liability and child sexual-abuse material demonstrates the need for greater clarity within India's existing legal framework. The first and perhaps most important reform should be to clearly define the relationship between the reporting obligations under POCSO and the safe-harbour provisions governing online intermediaries. At present, platforms operate within a legal environment shaped by multiple statutes and regulatory rules, which can create uncertainty about when an intermediary's responsibility begins and what steps it is legally expected to take after becoming aware of potentially unlawful material. Clear statutory guidance would help platforms understand their obligations while also providing courts with a more consistent basis for determining liability. Such clarity is particularly important where criminal consequences may follow from a failure to report or respond appropriately.

At the same time, the principle of **safe harbor should not be abandoned.** Intermediary protection remains necessary because platforms cannot reasonably be expected to anticipate or prevent every piece of content uploaded by millions of users. However, safe harbour should continue to operate as a conditional protection rather than as an absolute shield. An intermediary that genuinely complies with applicable legal and due-diligence requirements should retain the benefit of that protection, whereas the mere invocation of intermediary status should not excuse a platform from complying with independent statutory duties once those duties have been triggered. The objective, therefore, should not be to transform every platform into a publisher, but to ensure that safe harbour does not become a mechanism for avoiding legally recognised responsibilities.

Indian law should also consider adopting a **capability-based approach to platform responsibility**. Not all digital platforms possess the same technological resources, user base, infrastructure or capacity to identify and respond to harmful material. A large platform with sophisticated artificial-intelligence systems, extensive content-moderation infrastructure and substantial control over the visibility and circulation of content cannot necessarily be treated in exactly the same manner as a small service provider with limited technical capacity. Greater technological capability should correspond with proportionately greater responsibility, particularly where the risks to children are foreseeable and substantial. Such an approach would allow the law to remain flexible while avoiding the unrealistic expectation that every intermediary must satisfy identical technological standards.

Another important reform would be the introduction of **Child-Safety Impact Assessments** for significant online platforms and high-risk artificial-intelligence services. Before deploying systems that are likely to be used by children or that may facilitate the generation, recommendation or circulation of harmful material, platforms should be encouraged or required to identify foreseeable child-safety risks and explain the safeguards they have adopted to address them. Such assessments could examine content-moderation mechanisms, recommendation systems, reporting procedures, age-related risks, AI-generation capabilities and mechanisms for responding to suspected CSEAM. The emphasis would thereby shift from responding to harm after it occurs towards anticipating and reducing foreseeable risks at the design stage.

The reliability of automated detection systems also requires greater attention. AI-based moderation can play an important role in identifying known CSEAM and assisting human moderators, but these systems are not infallible. False positives may result in lawful material being wrongly removed, while false negatives may allow harmful material to remain undetected. Independent auditing of high-risk moderation systems could therefore provide an important layer of accountability. Such audits should examine the accuracy and reliability of the technology, error rates, human-review mechanisms, escalation procedures, data governance and safeguards against misuse. Greater transparency in these areas would not only strengthen regulatory oversight but could also improve public confidence in the use of AI for child protection.

The preservation of digital evidence should also form part of the platform's legal responsibilities once a credible allegation of CSEAM arises. Digital material can be deleted, modified or redistributed within a very short period, and inadequate preservation practices may seriously affect subsequent investigation and prosecution. Platforms should therefore have clearly defined procedures for preserving relevant information in accordance with law, while ensuring that such preservation does not become an excuse for excessive or indefinite retention of users' personal data. The preservation framework must consequently be accompanied by clear limitations concerning access, retention periods and lawful disclosure.

At the same time, stronger monitoring of online platforms must not come at the cost of fundamental rights. Measures intended to detect child sexual-abuse material may involve the processing of highly sensitive information and could, if poorly designed, develop into forms of indiscriminate surveillance. India's constitutional commitment to privacy, particularly following the Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India, requires that child-protection measures remain necessary, proportionate and subject to appropriate safeguards. Protecting children and protecting privacy should therefore not be treated as competing objectives. A well-designed regulatory framework should seek to achieve both.

Finally, India's intermediary-liability framework must continue to evolve alongside developments in **generative artificial intelligence and synthetic media**. AI-generated sexual material involving children manipulated images of real children and increasingly sophisticated synthetic videos raise questions that traditional content-regulation frameworks were never designed to address. Future regulation will therefore need to consider not only how platforms respond to existing CSEAM but also how their technologies may facilitate the creation and circulation of new forms of abuse. The central challenge for Indian law is to develop a framework that is sufficiently strong to protect children, sufficiently precise to support meaningful accountability, and sufficiently flexible to respond to technological change without compromising constitutional rights.

XV. RETHINKING THE ROLE OF DIGITAL PLATFORMS

The debate over intermediary liability under POCSO reflects a broader change in the way digital platforms operate. Traditionally, an intermediary was understood as a relatively passive channel through which users communicated and shared information. That understanding is becoming increasingly difficult to sustain. Modern platforms do much more than simply transmit content. Through algorithms and artificial intelligence, they influence what users see, what content is recommended, what material is removed, which accounts are restricted and how information spreads across their networks.

This does not mean that every platform should be treated as a publisher or held responsible for everything uploaded by its users. Such an approach would be unrealistic and could undermine innovation and freedom of expression. At the same time, treating platforms as completely passive intermediaries may overlook the considerable technological control they exercise over the digital environment. A more balanced approach would require courts to examine the circumstances of each case, including what the platform knew, whether it had received credible information about unlawful material, what technological capabilities were available, and what degree of control it exercised and how it responded after becoming aware of the risk.

This approach becomes particularly important in relation to child sexual-abuse material. When such material is repeatedly circulated online, the platform's response can determine whether the harm is

contained or amplified. The issue is therefore not simply whether the platform created the material, but whether it acted responsibly once it knew, or reasonably should have known, about the risk.

Generative AI makes this question even more complex. Platforms can now generate, modify, recommend and filter content through automated systems. Responsibility must therefore increasingly consider not only the content itself but also the design, safeguards and governance of the technologies through which that content is produced and distributed.

These developments also have implications for **digital constitutionalism**. Private platforms increasingly influence how individuals exercise rights such as privacy, expression and access to information. The challenge for Indian law is to hold such technological power accountable without creating disproportionate restrictions. The future of intermediary liability should therefore be based on **proportionate responsibility**, linked to knowledge, capability, control, risk and compliance with clearly defined legal duties.

XVI. CONCLUSION

The Supreme Court's decision to examine whether online platforms can face prosecution under POCSO marks an important stage in the development of India's intermediary-liability framework. Although the proceedings do not establish automatic criminal liability for platforms, they bring several difficult questions to the forefront. At the heart of the debate is whether an intermediary can continue to rely on safe-harbour protection when independent statutory duties under POCSO have been triggered, particularly where the platform has knowledge of abusive material and the technological ability to respond.

The Supreme Court's decision in Just Rights for Children Alliance v. S. Harish has already shown that legal concepts such as possession and control must be understood in light of contemporary digital realities. The emerging question of platform responsibility takes this reasoning a step further. It requires the law to consider not only the conduct of individual users but also the role and capabilities of the technological systems through which harmful material is circulated.

Indian law should therefore avoid both extremes. Platforms should not be held criminally responsible simply because unlawful material appears somewhere within their services. Such an approach would be unrealistic and could undermine the rationale of intermediary safe harbour. At the same time, intermediary status should not become an indefinite shield where a platform has actual knowledge of serious unlawful activity, possesses meaningful technological capabilities and fails to comply with a clear legal obligation.

A more balanced approach is one of **proportionate responsibility**, where the extent of responsibility is assessed according to knowledge, capability, control and risk, while criminal liability remains dependent on clearly established statutory requirements and culpability. This approach can protect children without turning every technological failure into a criminal offence.

The challenge becomes even more urgent with the growth of generative AI. Synthetic CSEAM, manipulated images and AI-generated material involving children demonstrate that forms of digital abuse are evolving faster than traditional legal categories. India's regulatory framework must therefore continue to develop alongside these technologies, bringing together child protection, intermediary governance, AI accountability and constitutional safeguards.

Ultimately, the principle should be neither that platforms are publishers nor that they are immune from responsibility. **Digital power should carry corresponding legal responsibility.** The challenge for Indian law is to define that responsibility carefully enough to protect children while preserving privacy, freedom of expression, innovation and due process. The way this balance is achieved may shape not only the future of POCSO enforcement but also the broader direction of intermediary liability and AI governance in India.

REFERENCES

[1] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[2] Committee on the Rights of the Child. (2021). General comment No. 25 (2021) on children's rights in relation to the
digital environment. United Nations.
[3] Government of India. (2000). Information Technology Act, 2000. Ministry of Electronics and Information Technology.
[4] Government of India. (2012). Protection of Children from Sexual Offences Act, 2012. India Code.
[5] In Re: Prajwala, (2018) 10 SCC 65.
[6] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[7] Just Rights for Children Alliance & Anr. v. S. Harish & Ors., 2024 INSC 716.
[8] Ministry of Electronics and Information Technology. (2021). Information Technology (Intermediary Guidelines and
Digital Media Ethics Code) Rules, 2021. Government of India.
[9]Ministry of Electronics and Information Technology. (2026). Information Technology (Intermediary Guidelines and
Digital Media Ethics Code) Amendment Rules, 2026. Government of India.
[10] Ofcom. (2026a). Illegal content duties under the Online Safety Act. Office of Communications.
[11] Ofcom. (2026b). Protection of children duties under the Online Safety Act. Office of Communications.
[12] Ofcom. (2026c). Roadmap to regulation under the Online Safety Act. Office of Communications.
[13] Shreya Singhal v. Union of India, (2015) 5 SCC 1.