

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DIGITAL SEXUAL ABUSE OF CHILDREN: EMERGING CHALLENGES UNDER THE POCSO FRAMEWORK

AUTHORED BY - KISHORE CHIMMILI

Institute/Designation: SVD Siddhartha Law College Vijayawada

ABSTRACT

The migration of child sexual abuse from physical to digital spaces has exposed structural limitations in a statutory framework — the Protection of Children from Sexual Offences Act, 2012 (POCSO) — conceived principally to address contact and proximate offences. This paper undertakes a doctrinal and analytical examination of the challenges that digitisation poses to the POCSO framework, situating the Act within the wider matrix of the Information Technology Act, 2000, the Juvenile Justice Act, 2015, and the newly notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. It traces the Supreme Court's landmark September 2024 ruling in S. Harish v. State of Tamil Nadu, which overturned a widely criticised Madras High Court decision and held that mere viewing, downloading and storage of child sexual abuse material constitutes an offence under Section 15 of the POCSO Act and Section 67B of the Information Technology Act, 2000 — a ruling that also directed courts to abandon the term 'child pornography' in favour of 'Child Sexual Exploitative and Abuse Material' (CSEAM), better reflecting the abuse inherent in such material. The paper further examines the graded liability structure introduced by the 2019 Amendment to Section 15, the persistent definitional gap concerning artificial-intelligence-generated and deepfake material depicting children, and the intermediary due-diligence and takedown obligations introduced by the 2026 IT Rules for 'synthetically generated information'. Drawing on comparative material from recent United States prosecutions involving AI-generated abuse material, and on Parliamentary data showing a 94.47 per cent increase in registered POCSO cases between 2017 and 2023, the paper identifies encryption-driven detection gaps, cross-border jurisdictional limitations, under-utilisation of the mandatory reporting obligation under Sections 19 and 20, and definitional ambiguity surrounding synthetic content as the principal unresolved challenges. It concludes with recommendations for statutory clarification of AI-generated CSAM, strengthened intermediary

accountability, and institutional capacity-building to close the gap between an increasingly protective judicial posture and the practical realities of digital enforcement.

Keywords: POCSO Act 2012; Child Sexual Abuse Material; CSEAM; Section 67B Information Technology Act; deepfake; synthetically generated information; online child sexual exploitation; digital sexual abuse; *S. Harish v. State of Tamil Nadu*; India.

1. INTRODUCTION

The Protection of Children from Sexual Offences Act, 2012¹ was enacted as a comprehensive, gender-neutral, child-specific criminal statute, drawing its constitutional foundation from Articles 15(3), 21 and 39(e)-(f) of the Constitution of India.² Conceived at a moment when digital penetration among Indian children was comparatively limited, the Act's original architecture was calibrated principally toward proximate, contact-based offences — penetrative and non-penetrative sexual assault, sexual harassment, and the use of a child for pornographic purposes. The subsequent, rapid expansion of smartphone access, encrypted messaging, and — most recently — generative artificial intelligence has exposed this architecture to forms of harm that its 2012 drafters could not fully have anticipated: mass circulation of abuse material at negligible cost, algorithmically generated synthetic depictions of children who may not exist or may be composites of real children's likenesses, and abuse material hosted on servers wholly outside India's territorial jurisdiction.

This paper examines how the POCSO framework — read together with the Information Technology Act, 2000 and its 2026 amendment rules — has responded to this shift, and where the framework continues to strain against the realities of digitally facilitated abuse. Its immediate occasion is the Supreme Court's September 2024 judgment in *S. Harish v. State of Tamil Nadu*, a decision that reoriented the law's treatment of private viewing and possession of abuse material and mandated a wholesale terminological shift away from 'child pornography'. But the paper's ambition is broader: it asks whether the doctrinal correction achieved in *S. Harish* is matched by an enforcement architecture capable of detecting, attributing and prosecuting abuse that increasingly occurs behind encryption, across borders, and — most recently — through content that no camera ever recorded.

The paper proceeds in six further parts. Part 2 reviews the existing literature on digital child sexual abuse and the POCSO framework. Part 3 sets out the statutory and institutional architecture. Part 4 undertakes detailed analysis across six dimensions: the *S. Harish* reconstruction of liability and terminology; the graded Section 15/67B liability structure; the

underused mandatory reporting obligation; the deepfake and AI-generated CSAM problem; the 2026 IT Rules governing synthetically generated information; and structural enforcement barriers. Parts 5 to 7 present findings, recommendations and conclusion.

2. LITERATURE REVIEW

2.1 *Doctrinal Commentary on the Possession-Liability Controversy*

The most immediate body of literature engages with the sequence of decisions culminating in *S. Harish v. State of Tamil Nadu*. Commentators have extensively analysed the Madras High Court's January 2024 ruling³, which held that mere downloading and private viewing of abuse material, without publication or transmission, did not attract liability under Section 67B of the Information Technology Act, 2000 or Section 15(1) of the POCSO Act — a position the literature widely characterised as dangerously narrow, given its reliance on a similarly restrictive earlier Kerala High Court approach.⁴ The Supreme Court's reversal is treated in the literature as a watershed, both for its substantive holding — that the 'demand side' of abuse material consumption is itself criminally culpable — and for its symbolic reframing of terminology.

2.2 *Empirical Literature on Reporting Gaps*

A second strand, exemplified by Manoj et al.'s 2025 study in *Child Protection and Practice*, examines interpersonal cybercrime against children empirically, documenting that the mandatory reporting obligation under Sections 19 and 20 of the POCSO Act remains substantially under-utilised by intermediaries, educational institutions, and even healthcare providers, notwithstanding its unambiguous statutory language. This literature situates under-reporting as a structural, not merely doctrinal, failure — one that survives even a favourable judicial reading of the substantive offence provisions.

2.3 *Emerging Literature on AI-Generated Abuse Material*

A third, rapidly growing strand addresses the challenge posed by artificial intelligence to child-protection law generally. Comparative commentary on prosecutions such as *United States v. Haslach* and *United States v. Cody Prater* demonstrates that jurisdictions with mature CSAM statutes are only beginning to work out whether, and how, entirely computer-generated depictions of fictional or composite children fall within statutory definitions premised on the 'use of a child'. Indian commentary on the 2026 IT Amendment Rules situates the Rules' introduction of 'synthetically generated information' as India's first comprehensive attempt to

bring such content within a regulatory perimeter, though — as this paper argues in Part 4.4 — the Rules address platform-level intermediary conduct more directly than they resolve the underlying POCSO definitional question.

This paper builds on all three strands but offers, to the authors' knowledge, the first integrated treatment situating the S. Harish reconstruction of possession liability, the 2019 Amendment's graded Section 15 structure, and the 2026 IT Rules' synthetic-content regime within a single analytical account of the POCSO framework's digital-era stress points.

3. STATUTORY AND INSTITUTIONAL FRAMEWORK

'Child pornography' — now judicially disfavoured in favour of CSAM/CSEAM — is defined under Section 2(1)(da) of the POCSO Act as any visual depiction of sexually explicit conduct involving a child, including photographs, videos, and digitally or computer-generated images indistinguishable from an actual child. Section 13⁵ and Section 14⁶ criminalise the use of a child for pornographic purposes and prescribe escalating punishment where such use is coupled with penetrative or aggravated sexual assault. Section 15⁷, substantially reworked by the 2019 Amendment⁸, separately criminalises storage and possession of such material, independent of any act of production.

This POCSO framework operates alongside Section 67B of the Information Technology Act, 2000⁹, which specifically targets the electronic publication, transmission, browsing, downloading, advertisement, exchange and distribution of material depicting children in sexually explicit acts, and the Juvenile Justice (Care and Protection of Children) Act, 2015¹⁰, which provides the complementary institutional architecture for child protection and rehabilitation. Notably, the Bharatiya Nyaya Sanhita, 2023¹¹ does not independently criminalise CSAM, leaving the field occupied by the POCSO Act and Section 67B, though general provisions on sexual offences may apply cumulatively. The Digital Personal Data Protection Act, 2023¹² has incidental relevance through its heightened consent and processing requirements for children's personal data, though it is not designed as, and does not operate as, a child-sexual-abuse statute.

Institutionally, the National Commission for Protection of Child Rights exercises a statutory monitoring role¹³ and operates the POCSO e-Box¹⁴, a dedicated online complaint mechanism, while cross-border referrals are increasingly channelled through the National Cyber Crime Reporting Portal's integration with international clearing-house mechanisms.

Table 1: Layered Statutory Response to Digital Child Sexual Abuse Material

Statute / Instrument	Core Obligation Created	Primary Actor Addressed
POCSO Act, 2012, ss. 13-15	Criminalises production, use of a child, and graded storage/possession of CSAM	Individual offenders
POCSO Act, ss. 19-20	Mandatory reporting of knowledge of abuse or abuse material	Any person, media, hotel/hospital staff, service providers
IT Act, 2000, s. 67B	Criminalises electronic publication, transmission, browsing, downloading, exchange of CSAM	Individual offenders /online conduct
IT Rules, 2021 (as amended 2026)	Due diligence, detection, labelling and takedown obligations for synthetic and unlawful content	Intermediaries / platforms
Juvenile Justice Act, 2015	Institutional care, rehabilitation and child-friendly procedure	Child Welfare Committees, State institutions

4. ANALYSIS AND DISCUSSION

4.1 From 'Child Pornography' to CSEAM: The S. Harish Reconstruction

In *S. Harish v. State of Tamil Nadu*¹⁵, the Supreme Court confronted a Madras High Court ruling that had quashed criminal proceedings against a person found to have downloaded and stored CSAM on his device, on the ground that private, non-transmissive viewing fell outside the scope of Section 67B of the Information Technology Act, 2000 and Section 15(1) of the POCSO Act. The Supreme Court, in a judgment authored by Justice J.B. Pardiwala, held that this reading was 'atrocious' and legally unsustainable, and that Section 67B is not confined to publication or transmission but extends to browsing, downloading and possession in appropriate circumstances, read together with the graded storage offence under Section 15.¹⁶ The judgment's significance extends beyond its substantive holding. The Court directed all courts to discontinue use of the term 'child pornography' in judicial orders and judgments, endorsing 'Child Sexual Exploitative and Abuse Material' (CSEAM) as more accurately reflecting the abuse inherent in such material, and urged Parliament to consider statutorily substituting the term.¹⁷ The Court further reiterated the mandatory reporting obligations under Sections 19 and 20 of the POCSO Act, holding that social media intermediaries, despite playing a significant role in the dissemination of such material, had largely disregarded this statutory duty — a finding that anticipates the intermediary-focused reforms subsequently introduced

by the 2026 IT Rules discussed in Part 4.5.

Read alongside the earlier 'skin-to-skin' controversy — in which a differently constituted bench of the Bombay High Court had held that groping a minor's breast without direct skin contact did not constitute 'sexual assault' under Section 7 of the POCSO Act, a ruling the Supreme Court unanimously overturned in 2021, confirming that sexual intent, not the mode or degree of physical contact, is the statute's organising criterion — S. Harish forms part of a broader pattern in which High Courts have, on occasion, construed POCSO's protective provisions narrowly, only for the Supreme Court to restore an expansive, victim-centred reading consistent with the Act's protective purpose.

4.2 The Graded Liability Structure of Section 15 and Section 67B IT Act

The 2019 Amendment restructured Section 15 into three graded tiers¹⁸: failure to delete, destroy or report stored material without further transmission; storage for the purpose of transmission, display or distribution; and storage or possession for commercial purposes, with materially escalating punishment across the three tiers and enhanced punishment on repeat conviction for commercial exploitation. This graded structure — recommended in consultations preceding the 2019 Amendment¹⁹ — represents a deliberate legislative choice to distinguish culpability by the offender's proximity to circulation and commercial exploitation, rather than treating all storage as equivalent. The S. Harish judgment's holding that mere viewing and downloading attracts liability operates principally at the threshold (first) tier of this structure, meaning that even the least culpable tier of Section 15 liability now captures conduct the Madras High Court had placed entirely outside the statute's reach.

A residual difficulty concerns the interface between Section 15's graded thresholds and Section 67B of the Information Technology Act, which does not import an equivalent gradation and instead lists a single undifferentiated set of prohibited acts (publishing, transmitting, browsing, downloading, advertising, promoting, exchanging or distributing). Where an accused's conduct falls within the least culpable tier of Section 15 but simultaneously within the broader language of Section 67B, courts must reconcile potentially divergent sentencing consequences arising from prosecution under either or both provisions — an area in which post-S. Harish sentencing practice remains to be doctrinally settled.

4.3 Mandatory Reporting under Sections 19-20: An Underused Safeguard

Sections 19 and 20²⁰ impose an affirmative duty on any person with knowledge of an offence, or of the existence of abuse material, to report to the police or the Special Juvenile Police Unit,

extending explicitly to media personnel, hotel and hospital staff, and — most relevant to the digital context — persons owning or managing a photographic or computer facility or service. Empirical literature²¹ documents that this obligation, despite its breadth, is substantially under-utilised, particularly by digital service providers, a gap the Supreme Court in *S. Harish* expressly noted when observing that intermediaries had 'so far ignored' their reporting obligations under the Act.

The practical reasons for this gap are structural rather than purely attitudinal: platforms operating at national or global scale process content at a volume that renders manual, case-by-case identification of CSAM commercially and operationally difficult without automated detection tools (themselves imperfect and contested on privacy grounds), and the absence, prior to 2026, of a codified takedown timeline meant that even identified material could persist online for extended periods without meaningful regulatory consequence for the hosting platform.

4.4 The Deepfake and AI-Generated CSAM Problem

The POCSO Act's definitional architecture, including Section 2(1)(da)²², was drafted with an implicit assumption that abuse material depicts an actual, identifiable child who has been used, in some manner, in its creation. Generative artificial intelligence disrupts this assumption in at least two distinct ways: first, by enabling the creation of wholly synthetic depictions of children who do not correspond to any real, identifiable individual; and second— the more disturbing and legally cleaner case — by enabling the 'digital undressing' or sexualised alteration of lawfully obtained photographs of real, identifiable children, as illustrated by the prosecution in *United States v. Haslach*²³, where a teacher used AI tools to generate sexually explicit depictions of his own students from ordinary photographs.

Comparative jurisprudence offers a useful, if not directly binding, reference point. In *United States v. Cody Prater*²⁴, a federal court rejected a First Amendment challenge to the prosecution of purely AI-generated obscene material depicting child sexual abuse, holding that the law draws no meaningful distinction between AI-generated and authentic material for purposes of criminal liability — a position that, while decided under a different constitutional framework, is instructive for how Indian courts might eventually approach the question whether Section 2(1)(da)'s definition (which already extends to 'digitally or computer-generated images') is broad enough to capture wholly synthetic material not derived from any identifiable child's likeness.

The Indian position remains, as of mid-2026, doctrinally unresolved at the POCSO level: no

reported Supreme Court or High Court decision has yet directly construed Section 2(1)(da) in relation to wholly AI-generated, non-identifiable synthetic CSAM, leaving the question to be addressed, for now, principally through the intermediary-focused mechanism of the 2026 IT Rules examined in the following section — an important but partial substitute for direct statutory clarification of substantive criminal liability.

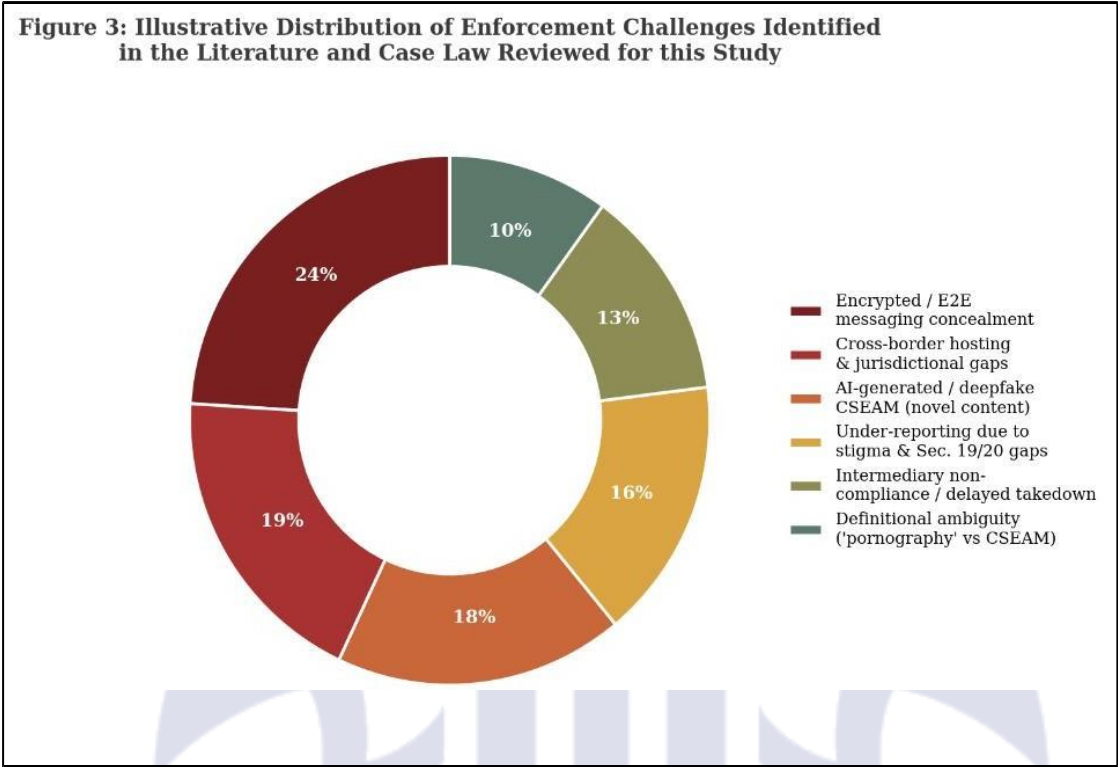


Figure 3. Illustrative distribution of enforcement challenges identified in the literature and case law reviewed for this study. Percentages reflect the relative frequency with which these challenges were foregrounded in the sources discussed in Parts 2 and 4, not a statistical survey of prosecutions.

4.5 The 2026 IT Rules: Regulating Synthetically Generated Information

On 10 February 2026, the Ministry of Electronics and Information Technology notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026²⁵, amending the 2021 IT Rules²⁶ to bring 'synthetically generated information' (SGI) within intermediaries' due diligence obligations for the first time. SGI is defined broadly as information that appears reasonably authentic but is artificially or algorithmically generated, modified, or altered using a computer resource²⁷, a formulation deliberately broad enough to capture AI-generated CSAM without requiring the underlying content to depict any identifiable real child — an approach that, while framed as platform

regulation rather than substantive criminal law, functionally closes part of the definitional gap identified in Part 4.4 by making platforms responsible for detecting and removing such content regardless of whether it depicts a real or synthetic child.

The 2026 Rules introduce a sharply compressed takedown timeline — reported at approximately two to three hours, down from the previous thirty-six-hour window — for flagged unlawful synthetic content acted upon pursuant to a court order or authorised government notice, applicable in particular to content that is sexually explicit or impersonating.²⁸ This timeline must be read against the constitutional framework established in *Shreya Singhal v. Union of India*²⁹, which confined intermediary 'actual knowledge' for safe-harbour purposes to notification through a court order or government notification under Section 79(3)(b) of the Information Technology Act — a precedent whose continuing relevance lies in ensuring that the accelerated takedown regime for CSAM-adjacent synthetic content does not, in its zeal for speed, dilute the due-process safeguards *Shreya Singhal* was designed to protect for other categories of contested online content.

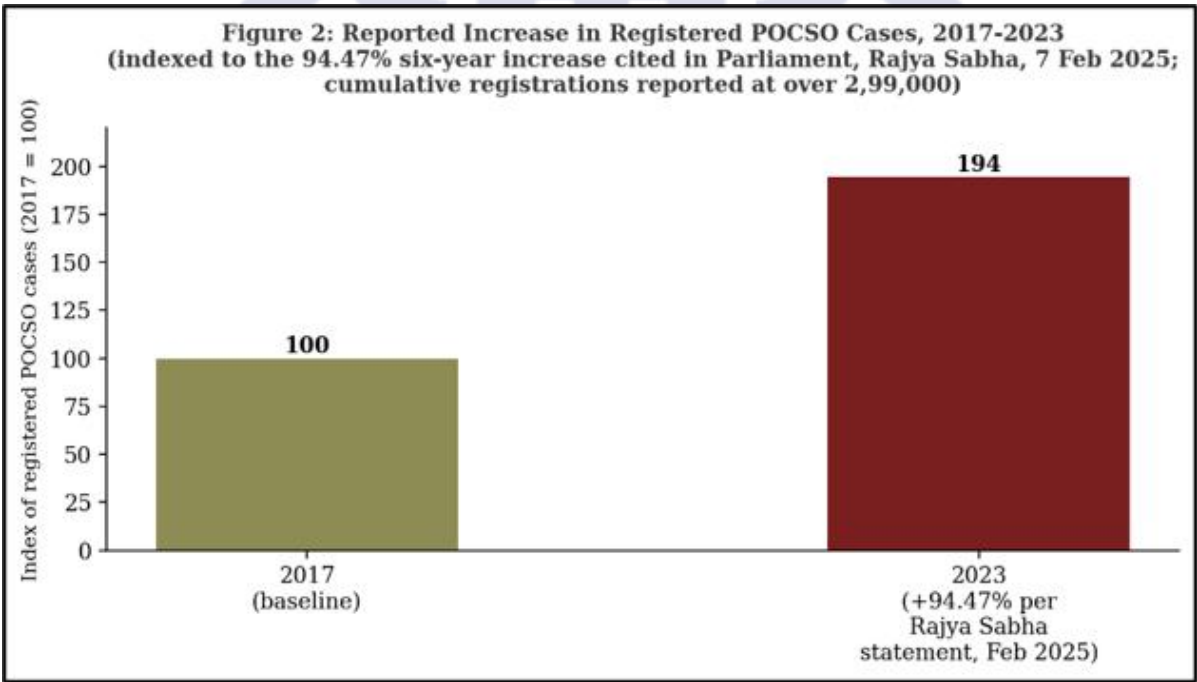


Figure 2. Reported increase in registered POCSO cases, 2017-2023, indexed to the 94.47% six-year increase cited in the Rajya Sabha on 7 February 2025. The underlying cumulative figure was reported at over 2,99,000 registered cases; the index presented here illustrates the scale of the reported increase rather than precise annual counts, which are not independently verified in this study.

4.6 Structural Enforcement Barriers: Encryption, Jurisdiction and Under-Reporting

Beyond the doctrinal and regulatory developments examined above, three structural barriers persist. First, end-to-end encrypted messaging platforms³⁰ continue to impede real-time detection and interception of CSAM in transit, since platform-side content scanning — the principal technical mechanism by which intermediaries identify such material for reporting under Sections 19-20 — is by design incompatible with true end-to-end encryption, creating an unresolved tension between privacy-protective encryption policy and child-protection detection imperatives. Second, cross-border hosting means that a substantial proportion of CSAM accessible to Indian users originates from, or is hosted on, servers outside India's territorial jurisdiction, requiring mutual legal assistance and international clearing-house cooperation³¹ that remains slower than the pace of digital circulation. Third, and relatedly, under-reporting³² by both platforms and individuals, driven by stigma, procedural unfamiliarity, and — prior to S. Harish — genuine doctrinal uncertainty about what conduct is even reportable, continues to depress the ratio of detected to actual incidents, a gap the Parliamentary statement citing a 94.47 per cent six-year increase in registered cases³³ may partly reflect improved detection and reporting rather than a proportionate increase in underlying incidence — a distinction the existing literature has not yet disentangled with confidence.

5. FINDINGS

Finding 1: S. Harish v. State of Tamil Nadu has substantially closed the possession-liability gap. By confirming that private viewing, downloading and storage of CSAM attracts liability under Section 15 of the POCSO Act and Section 67B of the Information Technology Act, the Supreme Court has foreclosed a demand-side loophole the Madras High Court's 2024 ruling had threatened to entrench.

Finding 2: Terminological reform (CSAM/CSEAM) is more than symbolic. The Court's direction to abandon 'child pornography' in judicial usage reframes such material as evidence of abuse rather than a form of pornography, with downstream implications for sentencing philosophy, victim characterisation, and public discourse, though the recommended statutory amendment substituting the term had not, as of mid-2026, been formally enacted.

Finding 3: The graded Section 15 structure and undifferentiated Section 67B liability are imperfectly reconciled. The 2019 Amendment's tiered culpability structure for storage offences is not mirrored in Section 67B of the Information Technology Act, creating potential inconsistency in how courts calibrate liability for conduct falling at the threshold of Section

15's three tiers.

Finding 4: Mandatory reporting under Sections 19-20 remains significantly under-enforced, particularly by digital intermediaries, a gap the Supreme Court itself identified in *S. Harish* and which the 2026 IT Rules' compressed takedown timelines address only partially, since a takedown obligation triggered by a court order or government notice presupposes that the material has already been detected and flagged through some other mechanism.

Finding 5: AI-generated and deepfake CSAM exposes a genuine, unresolved definitional gap in the POCSO Act. Section 2(1)(da)'s definition, while textually broad enough to include 'digitally or computer-generated images', has not yet been judicially tested against wholly synthetic, non-identifiable child depictions, leaving the 2026 IT Rules' intermediary-focused 'synthetically generated information' regime as a partial, platform-level substitute for direct statutory or judicial clarification of substantive criminal liability.

Finding 6: Encryption, cross-border hosting, and under-reporting remain the dominant structural — as opposed to doctrinal — barriers to enforcement, and are largely unaddressed by either the *S. Harish* ruling or the 2026 IT Rules, both of which operate principally at the level of domestic platform conduct and individual criminal liability rather than cross-border detection infrastructure.

6. RECOMMENDATIONS

- 1. Statutory Codification of CSEAM Terminology.** Parliament should give legislative effect to the Supreme Court's direction in *S. Harish* by formally substituting 'child pornography' with 'Child Sexual Exploitative and Abuse Material' throughout the POCSO Act and consequential amendments to the Information Technology Act, removing reliance on judicial direction alone for a terminological reform of continuing evidentiary and sentencing significance.
- 2. Explicit Statutory Recognition of AI-Generated and Synthetic CSAM.** Section 2(1)(da) of the POCSO Act should be amended to expressly clarify that its definition of prohibited material extends to wholly computer-generated or AI-synthesised depictions of a child engaged in sexually explicit conduct, irrespective of whether the depiction corresponds to an identifiable real child, aligning substantive criminal liability with the platform-level 'synthetically generated information' regime already introduced by the 2026 IT Rules.
- 3. Harmonisation of Section 15 POCSO and Section 67B IT Act Liability Tiers.** The Ministry of Home Affairs and Ministry of Electronics and Information Technology

should jointly issue clarificatory guidelines, or Parliament should amend Section 67B, to align its undifferentiated prohibition with the three-tier graded culpability structure of Section 15 POCSO, ensuring consistent sentencing outcomes for materially different degrees of culpability.

4. **Mandatory Automated Detection Obligations for Significant Intermediaries.** The 2026 IT Rules' due diligence framework should be supplemented with a specific, auditable obligation for significant social media intermediaries to deploy CSAM-detection technology (such as hash-matching against known abuse-material databases) as a condition of continued safe-harbour protection, with periodic compliance reporting to an appropriate regulatory authority.
5. **Strengthened Cross-Border Cooperation Mechanisms.** India should expand formal integration between the National Cyber Crime Reporting Portal and international clearing-house mechanisms, and pursue expedited mutual legal assistance protocols specifically for CSAM-related requests, recognising that a significant proportion of material accessible to Indian users is hosted outside India's territorial jurisdiction.
6. **Institutionalised Reporting Channels within Educational and Healthcare Settings.** The mandatory reporting obligation under Sections 19-20 should be operationalised through mandatory annual training and institution-level reporting protocols for schools, hospitals, and photographic/computer service providers, closing the awareness gap identified in the empirical literature and by the Supreme Court in *S. Harish*.
7. **Periodic, Disaggregated Data Publication.** The National Crime Records Bureau should publish annual, disaggregated data distinguishing contact-offence POCSO registrations from purely digital/CSAM-related registrations, enabling researchers and policymakers to determine whether reported increases (such as the 94.47 per cent six-year rise cited in Parliament) reflect rising incidence, improved detection, or a combination of both — a distinction the current literature cannot reliably draw from existing published statistics.

7. CONCLUSION

The POCSO framework has demonstrated a genuine, if incremental, capacity for judicial self-correction in the face of digital-era challenges. *S. Harish v. State of Tamil Nadu* closed a demand-side loophole that threatened to normalise private consumption of abuse material, and its accompanying terminological reform signals a judiciary increasingly attentive to the framing, and not merely the punishment, of digitally facilitated child sexual abuse. The 2019

Amendment's graded Section 15 liability structure and the 2026 IT Rules' introduction of a 'synthetically generated information' regime further demonstrate that both Parliament and the executive have begun to grapple, however imperfectly, with the scale and technological sophistication of contemporary offending.

Yet the framework's digital-era stress points are not fully resolved. The POCSO Act's core definitional provision has not been judicially or legislatively tested against wholly synthetic, AI-generated abuse material that depicts no identifiable real child — a gap the 2026 IT Rules address only at the level of platform conduct, not substantive criminal liability. The mandatory reporting obligation that both the Supreme Court and the empirical literature identify as chronically under-utilised remains without a specific, auditable enforcement mechanism. And the structural barriers of encryption, cross-border hosting, and detection-versus-incidence ambiguity in the underlying statistics remain largely untouched by either judicial correction or the most recent regulatory reform. Closing these gaps — through the statutory clarifications and institutional measures proposed in Part 6 — is the necessary next phase if India's protective jurisprudence for children is to keep pace with the technology increasingly used to exploit them.

REFERENCES

A. Statutes, Rules and Legislative Materials

1. *The Protection of Children from Sexual Offences Act, 2012 (No. 32 of 2012), as amended by the Protection of Children from Sexual Offences (Amendment) Act, 2019 (No. 25 of 2019).*
2. *The Information Technology Act, 2000 (No. 21 of 2000), s. 67B, as inserted by the Information Technology (Amendment) Act, 2008.*
3. *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.*
4. *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette Notification G.S.R. 120(E), 10 February 2026.*
5. *The Juvenile Justice (Care and Protection of Children) Act, 2015 (No. 2 of 2016).*
6. *The Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023).*
7. *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).*
8. *The Constitution of India, 1950, Arts. 15(3), 21, 39(e)-(f).*
9. *The Protection of Children from Sexual Offences (Amendment) Bill, 2024 (Private Member's Bill, Rajya Sabha, 2025).*

10. *Rajya Sabha, Debate on the Protection of Children from Sexual Offences (Amendment) Bill, 2024, 7 February 2025.*

B. Table of Cases

1. *Attorney General for India v. Satish*, 2021 SCC OnLine SC 1076.
2. *S. Harish v. Inspector of Police*, Crl. O.P. No. 3742 of 2024 (Madras High Court, 11 January 2024).
3. *S. Harish v. State of Tamil Nadu*, Criminal Appeal Nos. 2161-2162 of 2024, 2024 INSC 716.
4. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
5. *United States v. Cody Prater* (D. Kan. 2026).
6. *United States v. Haslach* (E.D. filing, 2025).

C. Books, Reports and Journal Articles

1. Daniel Manoj, Ranjit Immanuel James, Senthil Kumaran, Gerard Pradeep Devnath, Benjy Tom Varughese, Antony L. Arakkal and Latif Rajesh Johnson, 'Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation' (2025) 4 *Child Protection and Practice* 100088.
2. Freshfields Bruckhaus Deringer, 'India Targets Deepfakes and AI-Generated Content: Key Changes under MeitY's 2026 Amendments to the IT Rules' (2026).
3. InsightsonIndia, 'UPSC Editorial Analysis: Supreme Court's Ruling on Online Child Sexual Abuse' (2025).
4. Managing Intellectual Property, 'Regulating Synthetically Generated Information: India Amends IT Intermediary Rules' (2026).
5. Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C), Annual Report (2024-25).
6. Ministry of Women and Child Development, Government of India, and National Commission for Protection of Child Rights, Joint Consultation Report on Strengthening the POCSO e-Box and Cyber Reporting Mechanisms (2023-24).
7. Mondaq, 'IT Rules 2026 Deepfake Regulation: Three Hour Takedowns and AI Labelling Obligations' (2026).
8. National Commission for Protection of Child Rights, POCSO e-Box (online complaint mechanism).
9. Supreme Court Observer, 'Supreme Court's Landmark POCSO Judgement' (2024).

¹The Protection of Children from Sexual Offences Act, 2012 (No. 32 of 2012), Preamble.

²The Constitution of India, Arts. 15(3), 21, 39(e) and (f); the Act draws its constitutional foundation from the special protective power in favour of children and the Directive Principles mandating protection of childhood against exploitation.

³S. Harish v. Inspector of Police, Crl. O.P. No. 3742 of 2024 (Madras High Court, 11 January 2024), holding that mere downloading and private viewing of child sexual abuse material did not attract liability under s. 15(1) of the POCSO Act or s. 67B of the Information Technology Act, 2000 — subsequently overturned in S. Harish v. State of Tamil Nadu, 2024 INSC 716.

⁴See the earlier Kerala High Court ruling (discussed and disapproved in S. Harish v. State of Tamil Nadu, 2024 INSC 716) that watching an obscene photo or video by itself, without more, was not an offence under the relevant provisions.

⁵The Protection of Children from Sexual Offences Act, 2012, s. 13 (use of child for pornographic purposes).

⁶The Protection of Children from Sexual Offences Act, 2012, s. 14 (punishment for using a child for pornographic purposes).

⁷The Protection of Children from Sexual Offences Act, 2012, s. 15 (punishment for storage of pornographic material involving a child), as substituted by the POCSO (Amendment) Act, 2019, creating graded liability for storage without deletion/reporting, storage for transmission, and storage for commercial purposes.

⁸The Protection of Children from Sexual Offences (Amendment) Act, 2019 (No. 25 of 2019); Statement of Objects and Reasons noting the need to address the production and circulation of child pornography and child sexual abuse material through digital means.

⁹The Information Technology Act, 2000, s. 67B (punishment for publishing or transmitting material depicting children in sexually explicit act, etc., in electronic form), inserted by the Information Technology (Amendment) Act, 2008.

¹⁰The Juvenile Justice (Care and Protection of Children) Act, 2015 (No. 2 of 2016), read with the POCSO Act as complementary child-protection legislation.

¹¹The Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023), which does not independently criminalise child pornography, leaving the field occupied by the POCSO Act and s. 67B of the Information Technology Act, 2000, though relevant provisions on sexual offences and criminal intimidation may apply cumulatively in appropriate cases.

¹²The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), which, while primarily a data-protection statute, has incidental relevance to the processing of children's personal data online under s. 9.

¹³The Protection of Children from Sexual Offences Act, 2012, s. 44, read with the Commissions for Protection of Child Rights Act, 2005, s. 13, empowering the National Commission for Protection of Child Rights (NCPCR) to monitor the implementation of the Act; the NCPCR intervened as amicus in S. Harish v. State of Tamil Nadu, 2024 INSC 716.

¹⁴National Commission for Protection of Child Rights, POCSO e-Box: an online complaint mechanism enabling children to report sexual abuse, including digitally facilitated abuse, directly to the Commission.

¹⁵S. Harish v. State of Tamil Nadu, Criminal Appeal Nos. 2161-2162 of 2024, 2024 INSC 716 (Supreme Court, 23 September 2024), popularly the 'Just Rights for Children Alliance' judgment.

¹⁶S. Harish v. State of Tamil Nadu, 2024 INSC 716, paras 60-74 (holding that s. 67B of the Information Technology Act, 2000 is not confined to publication or transmission and extends to browsing, downloading and possession in appropriate circumstances, read with s. 15 of the POCSO Act).

¹⁷S. Harish v. State of Tamil Nadu, 2024 INSC 716, paras 45-52 (directing courts to replace the term 'child pornography' with 'Child Sexual Exploitative and Abuse Material' (CSEAM) or 'Child Sexual Abuse Material' (CSAM) in judicial orders, and recommending that Parliament amend the POCSO Act accordingly).

¹⁸The Protection of Children from Sexual Offences Act, 2012, s. 15(1)-(3) (as substituted in 2019), creating three graded offences: (i) failure to delete, destroy or report material without transmission (up to three years' imprisonment or fine or both); (ii) storage for transmission, display or distribution (three to five years or fine or both); and (iii) storage or possession for commercial purposes (three to five years and fine, on the second or subsequent conviction, three to seven years and fine).

¹⁹Law Commission of India and Ministry of Women and Child Development, Government of India, consultations preceding the 2019 Amendment to the POCSO Act, recommending graded penal provisions for storage, transmission and commercial exploitation of child sexual abuse material.

²⁰The Protection of Children from Sexual Offences Act, 2012, ss. 19 and 20, imposing a mandatory reporting obligation on any person (including media personnel, hotel and hospital staff, and photographic or computer-

related service providers) who has knowledge of the commission of an offence or of child pornographic material.

²¹Daniel Manoj et al., 'Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation' (2025) 4 Child Protection and Practice 100088.

²²The Protection of Children from Sexual Offences Act, 2012, s. 2(1)(da) (definition of 'child pornography', inserted by the POCSO (Amendment) Act, 2019, No. 25 of 2019).

²³United States v. Haslach (E.D. filing, 2025), a prosecution for the use of generative AI tools to create sexually explicit depictions of identifiable minors from lawfully obtained photographs ('digital undressing'), cited comparatively to illustrate the emergence of AI-facilitated child sexual abuse material generated from images of real, identifiable children.

²⁴United States v. Cody Prater (D. Kan. 2026), a federal jury verdict convicting the defendant for receipt and possession of authentic and AI-generated child sexual abuse material, the court having rejected a First Amendment challenge to the prosecution of purely AI-generated obscene material depicting minors — cited comparatively for its bearing on the treatment of synthetic CSAM.

²⁵The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified by the Ministry of Electronics and Information Technology, Gazette Notification G.S.R. 120(E), 10 February 2026, effective 20 February 2026.

²⁶The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under ss. 79 and 87(2) of the Information Technology Act, 2000.

²⁷The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, defining 'synthetically generated information' as information that appears reasonably authentic but is artificially or algorithmically generated, modified or altered using a computer resource, integrated into the due diligence framework of Rule 3 and new Rule 21(A).

²⁸The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 3(2), prescribing a takedown timeline (reported at approximately two to three hours, down from the earlier thirty-six-hour window) for flagged unlawful synthetically generated content acted upon pursuant to a court order or authorised government notice, applicable to content that is sexually explicit, impersonating, defamatory, or likely to incite violence.

²⁹Shreya Singhal v. Union of India, (2015) 5 SCC 1, on the constitutional limits of intermediary liability and the requirement of 'actual knowledge' through a court or government order under s. 79(3)(b) of the Information Technology Act, 2000 — a precedent of continuing relevance to the design of the 2026 takedown obligations for synthetic child sexual abuse material.

³⁰See generally, Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C), Annual Report (2024-25), on the challenges posed by end-to-end encrypted platforms to detection and interception of child sexual abuse material.

³¹Ministry of Home Affairs, Government of India, National Crime Records Bureau, Annual Report on the National Cyber Crime Reporting Portal and its integration with the National Center for Missing & Exploited Children (NCMEC) CyberTipline referral mechanism for cross-border reports of online child sexual abuse material.

³²See generally, Manoj et al. (2025) 4 Child Protection and Practice 100088, on jurisdictional and cross-border enforcement gaps in prosecuting offshore-hosted child sexual abuse material accessible to Indian users.

³³Rajya Sabha, Unstarred Question, 7 February 2025 (statement of Dr Fauzia Khan, MP, moving the Protection of Children from Sexual Offences (Amendment) Bill, 2024), citing National Crime Records Bureau data showing a 94.47% increase in registered POCSO cases over the six years since 2017, with cumulative registrations exceeding 2,99,000.