

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Cyber-Trafficking and Algorithmic Dehumanization: Critiquing the Bharatiya Nyaya Sanhita, 2023

DR. TANYA MITTAL* AND MADHAV BANSAL**

ABSTRACT

The intersection of advanced generative artificial intelligence, decentralized autonomous software, and organized crime networks has fundamentally altered the structural mechanics of child trafficking and sexual exploitation in India. This paper introduces the concept of the Cyber-Trafficking Nexus to evaluate the systemic transition from physical, geography-dependent human trafficking corridors to automated, borderless digital pipelines. It focuses on the phenomenon of “algorithmic dehumanization”, specifically the use of autonomous AI-enabled conversational agents for online child grooming, the deployment of machine-learning scrapers for targeting vulnerable demographics, and the automated production of synthetic Child Sexual Abuse Material (CSAM). By analyzing these technological shifts against India’s recently implemented penal codes, the paper exposes a critical legislative mismatch. It demonstrates that while Section 143 of the Bharatiya Nyaya Sanhita (BNS), 2023, establishes strict liability for child trafficking, its underlying statutory vocabulary remains bound to an analogue paradigm that presumes physical actions and human-to-human interaction. Furthermore, the study evaluates the procedural limitations of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and Section 67B of the Information Technology Act, 2000, regarding digital evidence collection and electronic cross-border jurisdictions. It concludes by proposing a comprehensive techno-legal regulatory matrix to enforce algorithmic accountability and structural cross-jurisdictional reform.

Keywords: Cyber-Trafficking Nexus, Bharatiya Nyaya Sanhita, Algorithmic Dehumanization, Synthetic CSAM, Autonomous Grooming

I. INTRODUCTION

In tracing the mechanisms through which sovereign power and legal order come to act upon human existence itself, Michel Foucault described the emergence of biopolitics: a shift in which the calculations of law and government moved from the discipline of individual bodies to the regularization and management of biological life as a population-level object.¹ Giorgio

* Author is affiliated with the Department of Laws, Panjab University, Chandigarh, India.

** Author is affiliated with the Department of Laws, Panjab University, Chandigarh, India.

¹ MICHEL FOUCAULT, THE HISTORY OF SEXUALITY, VOLUME I: AN INTRODUCTION (Robert Hurley tr, Vintage Books 1990) 139-43.

Agamben pressed that account further. His figure of the *homo sacer* is the person placed outside the protective reach of the legal order and reduced to what Agamben calls “bare life”, an existence exposed to violence without the protection that the legal order nominally guarantees.² The instrument that produces that exposure, on Agamben’s account, is the “state of exception”: a space in which the formal legal order does not operate, yet which continues to sit within the nominal authority of the state.³

The constitutional and penal response to human trafficking in India has long been directed at pulling the victim out of precisely that space and restoring them to the protection of Articles 21 and 23.⁴ The sudden expansion of low-cost data ecosystems, however, combined with the proliferation of consumer-facing generative artificial intelligence (AI) and automated software, has produced something the drafters of those protections did not have to contemplate. When an autonomous conversational agent running on natural language processing models targets, profiles and cultivates a child across encrypted, peer-to-peer networks, the minor is drawn into a distributed environment that the geography-bound machinery of the state struggles to reach.⁵ The borrowed vocabulary should be read as analytical rather than accusatory. The space in question is not one the Indian state has chosen to vacate; it is one that a statutory vocabulary built for physical conduct does not yet describe.

This process, which the paper calls algorithmic dehumanization, isolates the victim within a technical environment governed by automated scripts. The child’s vulnerabilities are no longer assessed by a human handler; they are rendered as data points, mined and acted upon by automated systems.⁶ This paper describes the structural convergence of digital commerce ecosystems, machine-learning models and contemporary exploitation networks as the Cyber-Trafficking Nexus.

The argument advanced here is that because Section 143 of the Bharatiya Nyaya Sanhita (BNS), 2023, remains tied to an analogue understanding of physical, human-to-human action, it is poorly equipped to reach conduct of this kind.⁷ Read through a techno-legal lens, algorithmic dehumanization sits awkwardly against the conventional understanding of *actus reus* and *mens*

² GIORGIO AGAMBEN, *HOMO SACER: SOVEREIGN POWER AND BARE LIFE* (Daniel Heller-Roazen tr, Stanford University Press 1998) 71-74.

³ GIORGIO AGAMBEN, *STATE OF EXCEPTION* (Kevin Attell tr, University of Chicago Press 2005) 1-6.

⁴ INDIA CONST. arts 21, 23. See also UPENDRA BAXI, *THE CRISIS OF THE INDIAN LEGAL SYSTEM* (Vikas Publishing House 1982).

⁵ ELOVSET ALLAHVERDIYEV, *NEW CHALLENGES OF COMBATING HUMAN TRAFFICKING IN THE DIGITALIZED WORLD* (2025).

⁶ NATIONAL HUMAN RIGHTS COMMISSION, INDIA, *Proceedings of the One-Day National Conference on Human Trafficking: Combating Human Trafficking in the Digital Era* (NHRC India 2025), held in collaboration with HIDAYATULLAH NATIONAL LAW UNIVERSITY, Raipur, 7 February 2025.

⁷ The Bharatiya Nyaya Sanhita 2023 (Act 45 of 2023), s 143.

rea carried forward into the new penal code, and that awkwardness is not merely academic: it is the space in which charging decisions are contested.⁸ The procedural framework of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and Section 67B of the Information Technology Act, 2000, compounds the difficulty, because enforcement organs remain organised along territorial lines.⁹ The paper therefore argues for a shift from a reactive, localized enforcement model to a technologically integrated, federally coordinated and survivor-centric system.¹⁰

II. THE CYBER-TRAFFICKING NEXUS: HOW DIGITAL PIPELINES REPLACE PHYSICAL CRIME

To understand why the criminal law strains, it is necessary first to describe how modern trafficking operates. Traditional trafficking relied on physical networks: local agents and intermediaries who identified, cultivated and moved victims. That infrastructure is increasingly replaced by what may be called a digital pipeline. Syndicates exploit the open internet, the dark web and mainstream social media platforms to automate stages of the offence that once required human presence, and in doing so they operate across borders at a scale and speed that human handlers could not achieve.

A. Automated Victim Identification

Sourcing was once a matter of physical presence in places where children gather. In the Cyber-Trafficking Nexus that stage is substantially automated. Automated collection tools, commonly described as web scrapers, are directed at public forums, educational websites and social media networks, where they gather and analyse the publicly visible digital traces of minors. The systems are configured to detect publicly expressed markers of distress or isolation, and the resulting profile allows a network to identify a child as a likely target without any person conducting a physical search. The consequence for enforcement is that the identification stage leaves almost no physical trace and generates no local complaint.

B. Artificial Intelligence in the Recruitment Phase

Once a child has been identified, the recruitment stage that historically required sustained human contact is increasingly handled by software. Conversational agents built on large

⁸ JUSTICE J.S. VERMA COMMITTEE, *Report of the Committee on Amendments to Criminal Law* (Government of India 2013), ch on trafficking of women and children (recording the assumption of bodily movement underlying the anti-trafficking provisions then proposed).

⁹ The Bharatiya Nagarik Suraksha Sanhita 2023 (Act 46 of 2023), ss 105, 185, read with the Information Technology Act 2000 (Act 21 of 2000), s 67B.

¹⁰ UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Global Report on Trafficking in Persons 2024* (United Nations 2024).

language models initiate and maintain contact through messaging services and chat environments. These systems reproduce age-appropriate registers of speech, adapt to emotional cues in the course of an exchange, and sustain contact over extended periods.¹¹ The National Center for Missing and Exploited Children recorded a 1,325 per cent increase in CyberTipline reports involving generative AI technology in 2024 as against 2023, out of a total of 20.5 million reports received that year, and a distinct category of those reports concerned chat-based exploitation.¹²

The shift matters for enforcement because it removes the constraints that previously limited the scale of the offence. A single operator can deploy many such agents concurrently, so that the temporal and geographic limits which once bounded an individual offender no longer apply. The initial phases of manipulation are dehumanized in a literal sense: no human being is present at the point of contact, and the child is isolated within a technical environment controlled by software rather than by an identifiable person.

C. The Production and Monetization of Synthetic CSAM

The final stage of the digital pipeline involves the generation and commercialization of synthetic child sexual abuse material (CSAM). Generative adversarial networks and diffusion models allow syndicates to manufacture realistic imagery, including material generated without any direct contact offence.¹³ Research on the training corpora of widely distributed image-generation models has also established that verified abuse imagery has been present in those corpora, which situates the problem upstream of the individual offender and within the model supply chain itself.¹⁴

Synthetic material of this kind is frequently deployed in financial sextortion, where a minor is coerced by threats to circulate the material within their own social network. Monetization is similarly automated, relying on darknet marketplaces, encrypted distribution channels and cryptocurrency payment rails, producing an illicit economy that operates at a considerable remove from any physical location that a district police force can search.

¹¹ NATIONAL HUMAN RIGHTS COMMISSION, INDIA (n 6).

¹² NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, *NCMEC Releases New Data: 2024 in Numbers* (8 May 2025).

¹³ David Thiel, Melissa Stroebel and Rebecca Portnoff, *Generative ML and CSAM: Implications and Mitigations* (STANFORD INTERNET OBSERVATORY and THORN, 24 June 2023).

¹⁴ David Thiel, *Identifying and Eliminating CSAM in Generative ML Training Data and Models* (STANFORD INTERNET OBSERVATORY, 20 December 2023).

III. STATUTORY GAPS: THE INTERACTION OF THE PENAL CODE, POCSO AND THE INFORMATION TECHNOLOGY ACT

The Bharatiya Nyaya Sanhita, 2023, was enacted to modernize substantive criminal law in India, and in several respects it does address technology directly. What matters in a trial court, however, is the operative statutory language, because that is the text against which a charge is framed and defended. Prosecuting online child exploitation ordinarily requires the combined use of the BNS, the Protection of Children from Sexual Offences (POCSO) Act, 2012, and the Information Technology (IT) Act, 2000. When those statutes are applied to conduct executed by automated systems, particular points of friction emerge. They are narrower than is sometimes claimed, but they are real, and they matter at the charging stage.

A. The Organised Crime Syndicate Threshold under the Penal Code

Section 111 of the Bharatiya Nyaya Sanhita creates a distinct offence of organised crime. Its opening subsection expressly extends to continuing unlawful activity in the nature of cyber-crimes and trafficking of persons, so the provision cannot be said to have overlooked the digital dimension of the problem.¹⁵ The difficulty lies elsewhere, in the definitional threshold. The Explanation to Section 111 defines an organised crime syndicate as a group of two or more persons who, acting singly or jointly as a syndicate or gang, indulge in continuing unlawful activity.¹⁶

The threshold is therefore a numerical one, and it is expressed in terms of persons. Cyber-trafficking does not always satisfy it. A single operator can write and deploy software that generates a large number of automated accounts which then carry out the identification and contact stages concurrently. If a prosecutor seeks to charge that operator under Section 111, the defence answer is straightforward: one person is not a group of two or more, and the automated accounts are instances of a program rather than members of a gang. The scale of the conduct is substantial, but the provision measures organisation by counting persons, and on that measure the conduct falls outside it. Whether the legislature intended that result, or simply did not anticipate the fact pattern, the drafting produces an outcome that is difficult to defend in policy terms.

B. Autonomous Systems and Sexual Harassment under the POCSO Act

Section 11 of the POCSO Act defines sexual harassment of a child, and does so through conduct verbs: a person commits the offence if, with sexual intent, he utters any word or makes any

¹⁵ The Bharatiya Nyaya Sanhita 2023, s 111(1).

¹⁶ *Ibid*, s 111, Explanation.

sound, or exhibits any object or part of the body, to a child, among other specified acts.¹⁷ The provision is drafted around an identified human actor performing an identified act.

Where the predatory text is generated by a large language model responding in real time to a child's messages, rather than typed by the accused, the defence will contend that the accused did not utter the words in question and that the specific output was not within his contemplation. Indian law is not without an answer. The doctrine of attribution recognised in *Iridium India Telecom Ltd. v. Motorola Inc.* allows the mental state of those who direct and control an enterprise to be attributed to the enterprise itself, on the footing that it thinks and acts through them.¹⁸ That doctrine, however, works by tracing intent back to a controlling human mind. Its logic is strained where the specific output was produced by a system operating on its own optimization, even though the decision to build, train and deploy that system for a predatory purpose was unmistakably human. The gap is not one of impunity so much as one of proof, and it falls on the prosecution.

C. Overriding Effect: The Information Technology Act and the POCSO Act

A further difficulty is said to arise where an accused creates or distributes synthetic CSAM, because two statutes appear to compete. The premise requires qualification at the outset. The definition of child pornography inserted into the POCSO Act by the 2019 amendment expressly extends to a photograph, video, digital or computer-generated image indistinguishable from an actual child, and to an image created, adapted or modified so as to appear to depict a child.¹⁹ Synthetic material is therefore squarely within the statutory definition. Any gap in relation to synthetic CSAM must be located in attribution, investigation and proof, not in the reach of the definition itself.

The apparent conflict of statutes is likewise narrower than it first appears. Publishing or transmitting material depicting children in sexually explicit acts is an offence under Section 67B of the IT Act.²⁰ Using a child for pornographic purposes, the punishment for it, and storage or possession of such material are offences under Sections 13, 14 and 15 of the POCSO Act.²¹ Section 81 of the IT Act contains a non obstante clause giving that Act effect notwithstanding anything inconsistent in any other law, subject to a proviso saving rights under the Copyright Act, 1957, and the Patents Act, 1970.²² It is Section 42A of the POCSO Act, and not Section 42,

¹⁷ The Protection of Children from Sexual Offences Act 2012 (Act 32 of 2012), s 11.

¹⁸ *Iridium India Telecom Ltd. v. Motorola Inc.*, (2011) 1 SCC 74.

¹⁹ The Protection of Children from Sexual Offences Act 2012, s 2(1)(da), inserted by the Protection of Children from Sexual Offences (Amendment) Act 2019 (Act 25 of 2019).

²⁰ The Information Technology Act 2000, s 67B.

²¹ The Protection of Children from Sexual Offences Act 2012, ss 13, 14, 15.

²² The Information Technology Act 2000, s 81 and proviso thereto.

that carries the corresponding overriding clause, providing that the POCSO Act is in addition to and not in derogation of other laws and prevails to the extent of any inconsistency.

Section 42 does something different, and it is dispositive of the concern most often raised. It provides that where an act constitutes an offence both under the POCSO Act and under specified provisions of the general penal law or under Section 67B of the IT Act, the offender shall be liable to punishment only under whichever of those laws provides for the greater degree of punishment.²³ The legislature has therefore already foreclosed the argument that an accused may be routed towards the lighter penalty of the IT Act. Read with Section 42A, the position is that the POCSO Act prevails on inconsistency and the heavier punishment prevails on sentence.²⁴ The Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish* confirms the practical point: proceedings under Section 15(1) of the POCSO Act and Section 67B of the IT Act were restored together, storage without any proof of transmission was held to be an offence, and the Court urged that the expression child pornography be replaced by child sexual exploitative and abuse material.²⁵

What survives of the criticism is narrower but not trivial. Section 42 identifies the competing general-law offences by their Indian Penal Code section numbers, and that enumeration has not been textually updated following the replacement of the Penal Code by the Bharatiya Nyaya Sanhita, so the comparison must now be routed through the repeal-and-savings machinery rather than read off the face of the section. That is a maintenance defect rather than a conflict of principle, but it is one that consumes time at the framing-of-charge stage in precisely the cases where time is most costly.

IV. CRITIQUING THE TRAFFICKING PROVISION OF THE BHARATIYA NYAYA SANHITA

The central difficulty of the Cyber-Trafficking Nexus lies in the distance between the technological reality of the conduct and the vocabulary of the substantive provision. Section 143 of the Bharatiya Nyaya Sanhita, 2023, is the principal anti-trafficking provision, and it carries forward the framework introduced into the Penal Code by the 2013 amendments, including graded punishment for the trafficking of a child and of more than one child, and repeat conviction. A close textual reading nevertheless suggests that it is poorly adapted to automated conduct.

²³ The Protection of Children from Sexual Offences Act 2012, s 42.

²⁴ *Ibid*, s 42A, inserted by the Criminal Law (Amendment) Act 2013 (Act 13 of 2013).

²⁵ *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716, [2024] 10 SCR 154.

A. Physical Verbs and Algorithmic Conduct

Section 143(1) provides that whoever, for the purpose of exploitation, recruits, transports, harbours, transfers or receives a person, by the specified means, commits the offence of trafficking.²⁶ Each of those verbs is drawn from a world of tangible action performed by a human agent in physical space.

Where a minor is identified by an automated collection tool hosted on a distributed cloud service, profiled by an algorithm and engaged by an autonomous agent, the application of those verbs becomes contestable. Does hosting an automated script on a remote server amount to harbouring? Does the routing of a child's profile across encrypted nodes amount to transporting? These are not rhetorical questions in a trial court. Penal provisions are construed strictly, and it is settled that where two reasonable constructions of a penal provision are available the court leans towards the one that does not extend criminal liability.²⁷ The consequence is that the ambiguity operates in favour of the operator of the software, which is precisely the outcome the provision should avoid.

B. Attributing Mens Rea to Autonomous Systems

A foundational proposition of criminal jurisprudence is *actus non facit reum nisi mens sit rea*: an act does not make a person guilty unless the mind is also guilty. Explanation 2 to Section 143 removes the consent of the victim from the inquiry altogether, and the graded sub-sections dealing with the trafficking of a child impose enhanced minimum punishment.²⁸ The prosecution must nevertheless establish that the accused acted for the purpose of exploitation, and it is that purposive element which the automation of the offence puts under pressure.

Where a system selects a target, generates the text of an approach and produces synthetic material without a contemporaneous human instruction directed at that child, the defence can characterise the outcome as an unforeseen consequence of deployment rather than a purposive act. The attribution doctrine remains available, and a court may legitimately find that the purpose was formed when the system was built, trained and released for that end.²⁹ But Indian penal law has no provision that says so expressly, and no codified framework of developer or deployer liability that closes the argument in advance. In practice the prosecution is left to construct from first principles what a statutory provision could state directly.

²⁶ The Bharatiya Nyaya Sanhita 2023, s 143(1).

²⁷ *Tolaram Relumal v. State of Bombay*, AIR 1954 SC 496.

²⁸ The Bharatiya Nyaya Sanhita 2023, s 143, Explanation 2, read with sub-ss (4)-(6).

²⁹ *Iridium India Telecom* (n 18).

V. PROCEDURAL AND JURISDICTIONAL BOTTLENECKS

Even where purposive conduct can be traced to a human operator, the enforcement machinery encounters procedural and territorial limits when it operates in a digital environment.

A. Digital Jurisdiction and the State List

The structural constraint is federal. Under Entries 1 and 2 of List II of the Seventh Schedule to the Constitution, public order and police are State subjects, so the statutory powers of a State police force stop at the State boundary.³⁰ A single course of trafficking conduct may nevertheless be distributed across several jurisdictions at once: the developer of the collection tool may operate from one State, the infrastructure hosting the conversational model from another, the child may reside in a third, and the wallet receiving the proceeds may sit outside India altogether. When a district Anti-Human Trafficking Unit begins to investigate, it encounters inter-State clearances and local warrants, and volatile digital records may be lost in the interval. The Union Government has moved to address the coordination problem, directing States to establish Anti-Human Trafficking Bureaus at police headquarters to link district units across State lines, but the underlying constitutional allocation is unchanged.³¹

B. Evidentiary Obstacles under the Procedure and Information Technology Statutes

The Bharatiya Nagarik Suraksha Sanhita, 2023, modernizes procedure in this area. Section 105 requires the process of search and seizure, including the preparation and signing of the seizure list, to be recorded through audio-video electronic means and forwarded without delay to the Magistrate, and Section 185 applies a comparable requirement to searches conducted by an investigating officer.³² Those provisions presuppose a seizable object: a device, a drive, a premises. Admissibility of what is recovered is now governed by Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which has replaced Section 65B of the Indian Evidence Act, 1872, and which requires certification of the electronic record.³³

The framework is less well suited to evidence that is volatile by design. Material distributed through ephemeral, end-to-end encrypted channels may leave no retrievable copy on the child's device. Section 67B of the IT Act, which criminalizes the publication and transmission of such

³⁰ INDIA CONST. sch VII, List II, entries 1, 2.

³¹ UNITED STATES DEPARTMENT OF STATE, *2024 Trafficking in Persons Report: India* (2024) (recording the March 2024 direction of the MINISTRY OF HOME AFFAIRS to States to establish Anti-Human Trafficking Bureaus at State police headquarters).

³² The Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 185.

³³ The Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023), s 63, replacing the Indian Evidence Act 1872, s 65B with effect from 1 July 2024.

material, depends in practice on cooperation from platforms and internet service providers.³⁴ Intermediaries have historically invoked user privacy and the proprietary character of their systems when asked for algorithmic logs, and delay in that exchange can be decisive. Defence counsel then contest admissibility on certification grounds under the Bharatiya Sakshya Adhiniyam, and the prosecution is left without the underlying record.

VI. JUDICIAL TRENDS AND THE PENDENCY PARADOX

The judicial approach to technology-facilitated offences against children reveals a contradiction between expansive interpretation and structural backlog. The higher judiciary has consistently widened protection. In *Independent Thought v. Union of India* the Supreme Court held Exception 2 to Section 375 of the Indian Penal Code unconstitutional insofar as it exempted sexual intercourse by a man with his wife between fifteen and eighteen years of age, holding that the marital relationship cannot dilute a girl child's protection.³⁵ In *Budhadev Karmaskar v. State of West Bengal* the Court issued directions under Article 142 to the police and to State governments concerning the treatment of sex workers, recording that many are victims of trafficking rather than offenders.³⁶ The latter decision does not concern children or technology, and it is cited here only for the narrower proposition that the Court has been willing to direct structural change in enforcement practice where legislation lags.

These directions collide with conditions in the trial courts. Even after the establishment of Fast Track Special Courts, including exclusive POCSO courts, disposal outcomes remain poor. The third-party evaluation of the scheme conducted by the National Productivity Council for the Department of Justice recorded conviction-to-disposal rates of 17.64 per cent in exclusive POCSO courts, 7.21 per cent in Fast Track Special Court cases and 5.54 per cent in regular court cases.³⁷ Whichever figure is taken, the outcome falls well short of what the scheme was designed to achieve.

Cyber-enabled elements compound the delay. Trial judges and prosecutors frequently lack specialized exposure to digital forensics, cloud architecture and the interpretation of algorithmic records, and the certification requirements attaching to electronic evidence give the defence a technical route to challenge admissibility. As a trial extends over years, retention periods expire,

³⁴ The Information Technology Act 2000, s 67B (n 20).

³⁵ *Independent Thought v. Union of India*, (2017) 10 SCC 800.

³⁶ *Budhadev Karmaskar v. State of West Bengal*, 2022 SCC OnLine SC 704 (order dated 19 May 2022).

³⁷ NATIONAL PRODUCTIVITY COUNCIL, *Third Party Evaluation of the Scheme on Fast Track Special Courts for Expeditious Disposal of Cases of Rape and POCSO Act* (report submitted to the DEPARTMENT OF JUSTICE, MINISTRY OF LAW AND JUSTICE, Government of India).

logs held outside the State are lost, and the child witness is exposed to prolonged secondary victimization, with attrition and acquittal the frequent result.

VII. PROPOSED REFORMS

Neutralizing the Cyber-Trafficking Nexus requires India to move from a fragmented, analogue enforcement model to a framework that is adapted to the technology actually in use.

A. Statutory Reconstruction: Codifying Algorithmic Criminal Liability

The legislature should amend Section 143 of the BNS, 2023, and Section 67B of the IT Act, 2000, so that the *actus reus* of trafficking expressly includes non-physical, automated conduct. The amendment should codify a framework of algorithmic criminal liability under which a person or corporate entity that knowingly develops, hosts or deploys automated collection tools or conversational models for exploitative or grooming purposes is treated as a principal offender, irrespective of whether any human-to-human interaction occurred. Codification would place on a statutory footing what courts can presently reach only through the attribution doctrine, and would remove the ambiguity on which the strict-construction argument depends. The threshold in the Explanation to Section 111 should be revisited for the same reason, so that organisation is measured by the scale and persistence of the operation rather than by counting human members.

B. Structural Centralization: A National Cyber-Trafficking Bureau

To address the limits of the State List allocation, the Union Government should consider a centrally empowered enforcement agency, provisionally a National Cyber-Trafficking Bureau, operating with statutory powers comparable to those of the National Investigation Agency in matters within its remit. Such a bureau would hold cross-border investigative jurisdiction over inter-State and transnational digital exploitation networks and would need permanent cyber-forensic capacity, data-analytics capability and standing channels for intelligence exchange with foreign enforcement agencies. Any such proposal must be reconciled with the constitutional allocation of police powers, which is a matter for Parliament rather than for administrative direction.

C. Intermediary Mandates and Algorithmic Auditing

Safe harbour under Section 79 of the IT Act should be conditioned on demonstrable compliance with child safety obligations.³⁸ Platforms, hosting providers and model developers should be required to deploy hash-matching tools and detection capable of intercepting automated

³⁸ The Information Technology Act 2000, s 79.

grooming behaviour and synthetic CSAM before transmission, and should be subject to periodic independent algorithmic audit so that optimization objectives do not, in effect, reward the amplification of youth vulnerability.

Part of this proposal has since been overtaken by regulation. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and brought into force on 20 February 2026, insert obligations in respect of synthetically generated information.³⁹ Rule 3(3) requires intermediaries to deploy reasonable and appropriate technical measures, including automated tools, to prevent the creation or dissemination of unlawful synthetic material; to label synthetic information prominently; to embed permanent provenance metadata carrying a unique identifier; and it prohibits the removal, suppression or modification of those labels and identifiers once applied.⁴⁰ The provenance obligation addresses the identification of synthetic material at scale, which is a significant advance. It does not, however, supply the proactive child-safety detection duty or the independent audit mechanism proposed here, and it operates on intermediaries rather than on the substantive criminal liability of the developer. The statutory amendments proposed above therefore remain necessary.

Taken together, these three interventions address the same defect at three levels. The rise of the Cyber-Trafficking Nexus represents a structural change in how the offence is committed, one that conventional, territory-bound legal regimes were not designed to meet. The enactment of the Bharatiya Nyaya Sanhita, 2023, is a significant act of codification, but its operative vocabulary in this area remains tied to an understanding of human interaction that the technology has moved past.

VIII. CONCLUSION

The intersection of generative artificial intelligence, automated software and organized crime has changed the character of human trafficking in India. As this paper has shown, the Cyber-Trafficking Nexus allows offenders to identify, cultivate and exploit children without physical proximity. Through automated collection tools and conversational agents, criminal networks achieve what is described here as algorithmic dehumanization: the reduction of a vulnerable child to a set of data points acted upon by software. The result is an environment in which the victim is isolated and in which territorially organized enforcement struggles to intervene.

³⁹ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E), notified 10 February 2026, in force 20 February 2026.

⁴⁰ *Ibid*, r 3(3).

The Bharatiya Nyaya Sanhita, 2023, was intended as a substantial step forward. This analysis suggests that in the specific field of technology-facilitated child exploitation its operative language has not kept pace. So long as Section 143 is framed around transporting and harbouring, and so long as Section 111 measures organisation by counting human members of a syndicate, automated conduct will continue to generate arguments that the provisions do not fit.

The interaction of the POCSO Act and the Information Technology Act is less problematic than is sometimes suggested, since Section 42 of the POCSO Act already directs that the greater punishment prevails and *S. Harish* has confirmed that concurrent prosecution is available. What remains is a maintenance defect in the enumeration within Section 42 and, more seriously, the practical burden of proving purposive human conduct behind an automated system. Where charge framing turns on whether a program can carry criminal intent, attention shifts away from the child, and trials extend while electronic records decay.

Reform should therefore be directed at three points. First, the substantive law should be amended to state expressly that creating, hosting or deploying automated systems for the purpose of grooming or exploiting a minor attracts the same liability as the corresponding physical conduct, and the definition of an organised crime syndicate should be revisited so that scale of operation, rather than headcount, determines the threshold.

Second, the enforcement architecture must be reconsidered. State police forces are bounded by their territorial jurisdiction, which is ill-suited to conduct distributed across servers in multiple jurisdictions. A centrally empowered agency with authority to investigate across State lines, trace digital financial flows and intervene against automated networks in real time would address that limitation, subject to the constitutional constraints noted above.

Third, the regulation of intermediaries requires further development. Platforms and model developers should not be able to rely on privacy or proprietary claims where their systems are used to reach children. The 2026 amendment to the Intermediary Guidelines has taken an important step in respect of the labelling and provenance of synthetic material; a proactive child-safety detection obligation and independent audit remain outstanding.

Until the vocabulary of the statute and the architecture of enforcement are brought into line with the technology in use, the constitutional guarantees of life and dignity will remain incompletely realised for the children this framework exists to protect. What is required is not new principle but drafting that reaches the conduct as it is now committed.
