Protecting Children in the Digital Era: A Critical Analysis of India's Legal Framework from POCSO to the Digital Personal Data Protection Act, 2023

Sakshi Bansal[1]

[1]Shobha Bhardwaj supervisor ITM University Gwalior

HOW TO CITE:
Sakshi Bansal (2026). Protecting Children in the Digital Era: A Critical Analysis of India's Legal Framework from POCSO to the Digital Personal Data Protection Act, 2023 International Journal of Special Education, 41(19s),1286 - 1298

ABSTRACT:

India's legal architecture for protecting children online has developed in disconnected layers rather than as a single, coherent scheme. The Protection of Children from Sexual Offences Act, 2012 was drafted for a world of physical proximity between offender and victim and had to be retrofitted through its 2019 amendment to reach the creation, storage and circulation of child sexual abuse material online. The Information Technology Act, 2000, principally through Sections 67, 67A and 67B and the Intermediary Guidelines of 2021, supplied the platform-facing obligations that POCSO itself does not impose. The Supreme Court's 2024 decision in *Just Rights for Children Alliance v. S. Harish* stitched these two statutes together for the first time in a single interpretive framework, while the constitutional recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India* supplied the doctrinal foundation for a data-protection statute that did not yet exist. That statute, the Digital Personal Data Protection Act, 2023, finally addresses a different but related harm: not the abuse of a child's image but the commercial exploitation of a child's data. This paper traces the four-stage evolution of criminal law, cyber law, constitutional law and data-protection law and argues that while each stage was individually necessary, their combined effect remains fragmented and supplements the analysis with primary survey evidence (N = 157) testing whether the gaps identified in the statutory text are also felt in practice. It argues that while each legislative stage was individually necessary, their combined effect remains fragmented. In conclusion the survey data corroborates from the perspective of parents, legal professionals, technologists and young people themselves. The paper concludes with recommendations for harmonizing enforcement across the Ministry of Home Affairs, the Ministry of Electronics and Information Technology and the forthcoming Data Protection Board of India. The notification of the Digital Personal Data Protection Rules, 2025 on 13 November 2025 operationalized for the first time statutory obligations on data fiduciaries regarding children's personal data, including a bar on behavioral tracking and targeted advertising directed at minors and a

requirement of verifiable parental consent. However, the phased implementation timeline - extending key obligations to November 2026 and May 2027 - means that meaningful protection remains prospective rather than actual. This paper undertakes a doctrinal, empirical and comparative legal analysis of the legislative continuum from POCSO (2012) through the Information Technology Act, the Juvenile Justice Act, 2015, to the DPDP Act, 2023 and DPDP Rules, 2025. It identifies definitional inconsistencies, the practical infeasibility of verifiable age-and-consent architecture and jurisdictional fragmentation among enforcement bodies as the principal weaknesses of the current regime. Drawing on comparative frameworks - the U.S. Children's Online Privacy Protection Act, the UK Age-Appropriate Design Code and Australia's Online Safety Act - the paper argues that statutory completeness on paper has outpaced institutional capacity to protect children in practice and proposes a converged, child-centric enforcement architecture to close this gap.

Keywords: POCSO Act; child sexual abuse material; Information Technology Act; Digital Personal Data Protection Act; child data privacy; Puttaswamy; intermediary liability

1. Introduction

The Indian child's experience of harm has been transformed by ubiquitous connectivity. Smartphones, ed-tech platforms, gaming applications andcial media have become primary sites of both socialization and risk for minors. Indian law has never had the luxury of designing child protection online from a blank page. Each statute in this field was written to answer the crisis of its own decade and each was then stretched sometimes uncomfortably to reach a threat that had not existed when it was drafted. The Protection of Children from Sexual Offences Act, 2012[1] (POCSO) was conceived to fill a long-standing gap in the Indian Penal Code which had no offence specifically addressing the sexual abuse of children.[2] It was not written with the internet in mind and had to be amended in 2019 to even name the phenomenon of digitally created and circulated abuse material.[3] The Information Technology Act, 2000[4] (IT Act) was in its original form, a law about electronic commerce and digital signatures; its child-specific provision, Section 67B, was inserted only by the 2008 amendment.[5] The constitutional right to privacy on which the entire edifice of data protection now rests was not settled law until 2017.[6] And the Digital Personal Data Protection Act, 2023[7] (DPDP Act) India's first comprehensive data protection statute and the first Indian law to condition the processing of a child's personal data on verifiable parental consent arrived only in August 2023, more than a decade after POCSO.

Empirical and anecdotal evidence increasingly suggests otherwise: online grooming, sextortion

[1] The Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012) (hereafter "POCSO Act").

[2] See Statement of Objects and Reasons, The Protection of Children from Sexual Offences Bill, 2011; India ratified the UN Convention on the Rights of the Child in 1992, creating an obligation to enact child-specific protective legislation.

[3] The Protection of Children from Sexual Offences (Amendment) Act, 2019 (Act No. 25 of 2019).

[4] The Information Technology Act, 2000 (Act No. 21 of 2000) (hereafter "IT Act").

[5] The Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009), inserting s 67B into the IT Act.

[6] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

[7] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (hereafter "DPDP Act").

and child sexual abuse material (CSAM) circulation typically begin with the routine, often consent-free, collection of a child's data - location, browsing behavior, contact lists and images - by applications with no meaningful safeguards for minors. The enactment of the Digital Personal Data Protection Act, 2023 and its long-awaited subordinate legislation, the Digital Personal Data Protection Rules, 2025 (notified on 13 November 2025) represents India's first attempt to treat children's data as a distinct category deserving heightened statutory protection. Yet this framework does not operate in isolation; it must be read alongside and reconciled with POCSO, the Juvenile Justice (Care and Protection of Children) Act, 2015 and the Information Technology Act's provisions on child sexual abuse material and intermediary liability.

II Research Objectives and Questions

2.1 Objectives

- To trace the legislative evolution of child protection law in India from POCSO (2012) through the IT Act, the Juvenile Justice Act, 2015, to the DPDP Act, 2023 and the DPDP Rules, 2025.
- To critically evaluate the adequacy of the 'verifiable parental consent' mechanism introduced under Section 9 of the DPDP Act, 2023 and elaborated in the DPDP Rules, 2025.
- To compare India's child-data-protection regime with leading international frameworks, including COPPA (United States), the UK Age-Appropriate Design Code and Australia's Online Safety Act, 2021.
- To assess the institutional and enforcement architecture governing child protection online, including the Data Protection Board of India, Special POCSO Courts, cybercrime authorities and the National Commission for Protection of Child Rights (NCPCR).
- To propose a harmonized, child-centric legal and institutional framework that bridges the current divide between offline child-protection law and online data-protection law.

2.2 Research Questions

- Does the DPDP Act's treatment of 'child' as any person below eighteen years create friction with narrower international thresholds such as COPPA's under-13 standard and what are the practical consequences of this divergence?
- Is 'verifiable parental consent', as contemplated under the DPDP Rules, 2025, operationally feasible given India's existing digital identity and age-verification infrastructure?
- Does the multiplicity of regulators - the Ministry of Electronics and Information Technology, the Data Protection Board, the NCPCR and law-enforcement agencies under POCSO and the IT Act - dilute accountability for child-related digital harm?
- What practical protection gap is created by the phased implementation timeline of the DPDP Rules, 2025 (extending certain obligations to November 2026 and May 2027)?
- What lessons can India draw from comparative frameworks to design a more coherent child-protection regime spanning both physical and digital harm?

III. Literature Review

Existing scholarship on this subject tends to specialize in one of the four regimes rather than tracing the line between them. Criminal law commentary on POCSO focuses heavily on sentencing severity and the 2019 amendment's introduction of the death penalty for aggravated offences generally treating the internet only as a vector for the underlying offline offence.[8] Cyber-law scholarship, by contrast, concentrates on intermediary liability under Section 79 of the IT Act and the 2021 Intermediary Guidelines, typically in the context of platform takedown obligations rather than the child-specific offence architecture in Sections 67A and 67B read together with POCSO.[9] Constitutional-law literature on *Puttaswamy* is voluminous but largely concerned with surveillance and Aadhaar and rarely draws the

[8] See, e.g., commentary summarized in Bhatt & Joshi Associates, "Protection of Children from Sexual Offences Act, 2012: A Comprehensive Legal Analysis" (2023), discussing the three-tier possession structure introduced under Section 15.

[9] See discussion of intermediary due diligence obligations in ASV Legal LLP, "Protection of Children from Online Harm: Assessing Legal Measures under the IT Act and POCSO Act" (2026).

connecting line to children's data specifically. Data-protection commentary on the DPDP Act, meanwhile, tends to analyze Section 9 and the DPDP Rules, 2025 in isolation from the criminal-law and cyber-law regimes discussed above, as though children's online safety and children's data privacy were unrelated fields of study.[10] This paper's contribution is to read all four regimes together as stages of a single evolving legislative response and to identify precisely where the seams between them create protective gaps.

Comparative privacy scholarship on COPPA and the UK Age-Appropriate Design Code offers extensive guidance on regulatory design choices, including risk-based tiering of obligations and 'privacy-by-default' settings for minors but has not yet been systematically mapped onto the Indian statutory landscape post-Rules.

This paper's contribution lies precisely at this intersection: it is among the first analyses to engage with the actual text and phased implementation schedule of the DPDP Rules, 2025, read jointly with pre-existing child-protection statutes, rather than treating child data protection as a standalone or purely prospective subject.

IV. Research Methodology

This paper adopts a doctrinal, black-letter method. It relies on primary sources and the POCSO Act and its 2019 amendment, the IT Act and the Intermediary Guidelines and Digital Media Ethics Code Rules, 2021, the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025, read alongside the leading constitutional and criminal judgments that interpret them principally *Puttaswamy* and *Just Rights for Children Alliance v. S. Harish*. Secondary sources as law-firm commentary, bar journal articles and advisories issued by statutory bodies such as the National Human Rights Commission is used to corroborate interpretation and to surface implementation gaps not visible from the bare text of the statutes. The paper does not undertake empirical or field research; its claims are limited to the coherence and interaction of the legal instruments themselves. The empirical component consists of a bilingual (English-Hindi) primary survey, The Privacy-Safety Paradox: Reconciling Child Rights in Digital India, administered as a self-administered online questionnaire and yielding 157 valid responses, routed through role-based branching logic into four stakeholder sets: parents/guardians, legal professionals, technology experts/educators and students reflecting on their own digital adolescence. 11 The survey was designed specifically to test, against direct stakeholder testimony, three doctrinal claims developed independently from the statutory and case-law analysis: that public awareness of DPDP Act rights remains uneven; that professional opinion on the adequacy of the current framework remains genuinely divided; and that self-declared age verification is structurally vulnerable to circumvention by the minors it is meant to constrain. The paper does not otherwise undertake empirical or field research; beyond the survey its claims are limited to the coherence and interaction of the legal instruments themselves.

V. The Foundational Framework

5.1 The Protection of Children from Sexual Offences Act, 2012

POCSO defines a child without gradation as any person below the age of eighteen and applies without distinction of gender to both victims and offenders.[11] Its core offences penetrative sexual assault, aggravated penetrative sexual assault, sexual assault and sexual harassment were at inception, framed around physical acts.[12] The provision most relevant to the digital context, Section 13, criminalizes the use of a child for pornographic purposes and was from the outset, broadly drafted to capture photographic, video and digital representations.[13] Yet it was only the 2019 amendment that gave the statute a working definition of "child pornography," extending it explicitly to digital and computer-generated images indistinguishable from an actual child and to images that have been created, adapted or modified to

[10] See, e.g., Chambers and Partners, "Child's Personal Data and Privacy: Analysing the Draft DPDP Rules, 2025" (17 February 2025), which analyses Rule 10 and Rule 11 without reference to POCSO or the IT Act.

[11] POCSO Act (n 1), s 2(1)(d).

[12] POCSO Act (n 1), ss 3-12.

[13] POCSO Act (n 1), s 13.

appear to depict one.[14]

The same amendment restructured Section 15 into a graded, three-tier offence covering possession and storage of such material: a lighter obligation to delete, destroy or report material found in one's possession; a heavier offence for storage with intent to transmit or distribute; and a still heavier offence for storage for commercial purposes.[15] This graded structure reflects a deliberate legislative choice to criminalize not only production and distribution but the demand side of the market: mere possession, even without further circulation, now attracts liability. Read together, Sections 13 to 15 make POCSO, at least on paper, one of the more stringent child sexual abuse material regimes among comparable jurisdictions.

POCSO defines a 'child' as any person below the age of eighteen years and criminalizes a broad spectrum of sexual offences, including penetrative and non-penetrative sexual assault, sexual harassment and the use of children for pornographic purposes. The 2019 amendment expanded the definition of 'child pornography' and enhanced penalties, reflecting legislative recognition that digital technology had become a vector for offences earlier conceived only in physical terms. POCSO further mandates the constitution of Special Courts for child-friendly trial procedures and establishes reporting obligations, including the National Commission for Protection of Child Rights' 'POCSO e-Box' for online complaint submission. However, POCSO's institutional design remains fundamentally criminal-justice oriented and is not equipped to regulate the routine, non-criminal collection and commercial exploitation of children's data that frequently precedes or facilitates such offences.

5.2 The Information Technology Act, 2000 and Intermediary Regulation

Section 67B of the Information Technology Act criminalizes the publication and transmission of material depicting children in sexually explicit acts and Section 79 provides a conditional safe harbor to intermediaries subject to due-diligence obligations. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose additional obligations on significant social media intermediaries, including proactive identification and removal of CSAM using automated tools. While these provisions address the circulation of harmful content, they do not regulate the upstream collection, storage, or commercial use of children's personal data by platforms with which children interact daily, such as educational and gaming applications - a gap the DPDP Act was intended to fill.

5.3 The Juvenile Justice (Care and Protection of Children) Act, 2015

The JJ Act operates alongside POCSO, defining a 'child in need of care and protection' and establishing Child Welfare Committees and Juvenile Justice Boards. Its relevance to digital harm is largely indirect, arising where online exploitation results in a child requiring institutional care or rehabilitation but it does not itself regulate digital data practices.

5.4 The Digital Personal Data Protection Act, 2023

Section 9 of the DPDP Act requires that a Data Fiduciary obtain verifiable consent from a parent or lawful guardian before processing the personal data of a child, defined as any person below eighteen years. The Act further prohibits processing of children's data that is likely to cause detrimental effect on their well-being and bars tracking, behavioral monitoring and targeted advertising directed at children. These provisions mark a conceptual departure from the earlier IT Act regime by treating children's data, as a category, as inherently more sensitive and deserving of default protective treatment rather than harm-based, after-the-fact regulation.

5.5 The Digital Personal Data Protection Rules, 2025

The DPDP Rules were notified by the Ministry of Electronics and Information Technology on 13 November 2025, together with a separate

[14] POCSO Act (n 1), s 2 as amended by the 2019 Amendment Act (n 3); see summary in Drishti Judiciary, "Important Definitions under POCSO Act, 2012".

[15] POCSO Act (n 1), s 15(1)-(3), as substituted by the 2019 Amendment Act (n 3); see Bhatt & Joshi Associates (n 8).

enforcement notification setting out a phased implementation timeline and the constitution of the Data Protection Board of India. Provisions relating to definitions, the Board's establishment and the Central Government's rule-making powers took immediate effect; obligations relating to registration and operation of consent managers become effective only after twelve months (13 November 2026); and certain remaining provisions are scheduled to take effect as late as May 2027. The Rules elaborate practical requirements for consent collection, breach notification, record-keeping and specifically address special protections for children and persons with disabilities. This phased design is significant for the present analysis: it means that, notwithstanding the DPDP Act's 2023 enactment, operative protection for children's data will not be fully realised in practice for several years after the underlying harms became legally cognizable.

VI. Extending Protection to Cyberspace: The IT Act, 2000 and the 2021 Intermediary Guidelines

That gap is filled, imperfectly, by the IT Act. Section 67 punishes the publication or transmission of obscene material in electronic form generally, while Section 67A does the same for sexually explicit material.[16] Section 67B is the child-specific provision and is considerably broader than its counterparts: it punishes not only the publishing and transmission of material depicting children in sexually explicit acts but also browsing and downloading such material and further criminalizes online grooming, inducing a child into a sexual act and facilitating child abuse through online means.[17] Its reach is, in this respect, wider than Section 13 of POCSO, since Section 67B criminalizes the act of viewing such material even where there is no intent to distribute or profit from it.

The IT Act's more distinctive contribution, however, lies in Section 79, which grants intermediaries social media platforms, internet service providers and hosting services conditional immunity from liability for third-party content, subject to their exercising due diligence.[18] The Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 operationalize that due-diligence standard specifically for child sexual abuse material: significant social media intermediaries must endeavor to deploy technology-based measures to proactively identify such material and all intermediaries must remove it promptly upon acquiring actual knowledge, whether through a court order or a government notification.[19] Failure to observe this due diligence costs the intermediary its safe-harbor protection under Section 79 and exposes it to liability under both the IT Act and POCSO, since courts have held that compliance with one statute does not absolve an intermediary of obligations under the other.[20]

VII. Judicial Consolidation: Just Rights for Children Alliance v. S. Harish (2024)

For over a decade, POCSO and the IT Act operated as parallel, loosely coordinated statutes. The Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish*, delivered on 23 September 2024, is the first authoritative attempt to read them as a single scheme. The case arose from a 2020 Cyber Tipline report identifying the respondent as a habitual consumer of child sexual abuse material; the Madras High Court had quashed the criminal proceedings against him on the reasoning that mere possession or viewing of such material, without an intent to transmit it further, did not amount to an offence under either POCSO or the IT Act.[21]

The Supreme Court reversed that finding. It held that Section 15(1) of POCSO independently penalizes the failure to delete, destroy or report

[16] IT Act (n 4), ss 67, 67A, both inserted by the Information Technology (Amendment) Act, 2008.
[17] IT Act (n 4), s 67B; see analysis in Apni Law, "Section 67B Information Technology Act, 2000" (2025).
[18] IT Act (n 4), s 79; the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; see Press Information Bureau, press release on Section 67B and the 2021 Rules; Bachpan India, "4 ways to prevent Child Sexual Abuse Material (CSAM)" (2024).
[20] See discussion of the interaction between Section 79 due diligence and POCSO reporting obligations in the Supreme Court's ruling discussed in Part VI below.
[21] S. Harish v State, Crl OP No 3465 of 2024 (Madras High Court, January 2024), quashing proceedings under Section 15 POCSO and Section 67B IT Act.

such material once found in one's possession, regardless of whether the possessor intended to share it and that Section 67B of the IT Act operates as a parallel, mutually reinforcing offence rather than a substitute for POCSO liability.[22] The Court went further than the facts of the case strictly required, holding that the due-diligence obligation under Section 79 of the IT Act includes an obligation to remove such material and report it to police in the manner POCSO itself specifies and that an intermediary's compliance with IT Act due diligence does not, by itself, discharge its separate obligations under POCSO.[23]In a further, terminology-focused intervention, the Court directed that the phrase "child pornography" be replaced in all judicial orders with "child sexual exploitative and abuse material" (CSEAM), on the reasoning that the former term risks implying consent and understates the severity of the underlying abuse.[24] This is the closest India's jurisprudence has come to treating POCSO and the IT Act as a single, coordinated child-protection code rather than two statutes that happen to overlap.

VIII. The Constitutional Bridge: Privacy, Puttaswamy and the Path to Data Protection

The regimes discussed so far address the abuse of a child's image or likeness. They say very little about a separate and increasingly significant harm: the routine commercial collection of a child's personal data browsing behavior, location, biometric identifiers, purchase history by platforms the child may lawfully use. That harm required a different doctrinal foundation and it was supplied by the Supreme Court's 2017 decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, in which a nine-judge bench unanimously held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21 of the Constitution.[25] Two features of that judgment matter directly for this paper. First, the Court expressly recognized informational privacy control over the collection, storage and dissemination of one's personal data as one of the distinct dimensions of the broader right, anticipating in doctrine a data-protection statute that India did not yet possess.[26] Second, the Court held that privacy is not absolute: any state measure restricting it must satisfy a threefold test of legality, legitimate aim and proportionality, the same test that later shaped the drafting of consent and purpose-limitation provisions in the DPDP Act.[27]

Puttaswamy did not itself create obligations for data fiduciaries, nor did it speak to children specifically. Without Puttaswamy, Section 9 of the DPDP Act would have lacked a settled constitutional anchor; with it, the child-specific consent architecture that follows can be read as a statutory elaboration of a right the Constitution already recognized.

IX. The Data Protection Layer: Section 9 of the DPDP Act, 2023 and the DPDP Rules, 2025 and Its Empirical Reception

Section 9 of the DPDP Act requires a Data Fiduciary to obtain verifiable consent from the parent or lawful guardian of a child again defined as anyone under eighteen before processing that child's personal data.[28] It separately and near-absolutely prohibits tracking, behavioral monitoring and targeted advertising directed at children. a prohibition that parental consent cannot cure.[29] The mechanics of "verifiable consent" were left to delegated legislation and were finally supplied by Rule 10 of the Digital Personal Data Protection Rules, 2025, notified on 13 November 2025, which permits verification either through details a fiduciary already holds because the parent is a registered user, or through a virtual token issued by a government-authorized digital locker service

[22] Just Rights for Children Alliance (n 15), discussing the graded structure of Section 15 POCSO and its relationship to Section 67B IT Act.
[23] Just Rights for Children Alliance (n 15); see also CyberPeace, "Supreme Court Landmark Ruling: CSEAM is an offence under POCSO and IT Act" (25 September 2024).
[24] Just Rights for Children Alliance (n 15); see O.P. Jindal Global University Child Rights Clinic, "Supreme Court Mandates Use of 'CSEAM' to Replace 'Child Pornography' in Legal Terminology" (2024).
[25] Puttaswamy (n 2).
[26] Puttaswamy (n 2), concurring opinion of Chelameswar J, stressing informational privacy and the need for a data protection law.
[27] Puttaswamy (n 2); the proportionality standard was further elaborated in Justice K.S. Puttaswamy v Union of India (Aadhaar) (2019) 1 SCC 1.
[28] DPDP Act (n 5), ss 9(1), 2(f).
[29] DPDP Act (n 5), s 9(3).

such as Digi Locker.[30] Rule 11 and the accompanying Fourth Schedule then carve out purpose-bound exemptions for clinical establishments, schools and childcare providers and for real-time location tracking undertaken strictly for a child's safety.[31]

It is worth being precise about what this layer does and does not add to the POCSO-IT Act framework discussed above. Section 9 is not concerned with sexual abuse material; it is concerned with the ordinary, often lawful, commercial processing of a child's data by the very platforms a child might use for school, entertainment or communication. The harm it targets behavioral profiling, algorithmic targeting, non-consensual data trading is real but categorically distinct from the harm POCSO and Section 67B address. That distinction and the absence of any statutory bridge between the two harms, is the central gap examined in Part IX.

To test whether the gaps identified in this statutory design are also felt in practice, the author supplemented the doctrinal analysis above with a primary bilingual (English-Hindi) survey drawing 157 valid responses, routed through built-in branching logic into four role-specific question sets: Parent/Guardian, Legal Professional, Technology Expert/Educator and Student, with a final set of questions put to the full sample regardless of role.[32] The sample skews young and highly educated: 73.2% of respondents were aged 1288-1299 and 78.3% held an undergraduate degree or higher.[33] By self-reported role, 53.5% identified primarily as students, 17.2% as parents or guardians, 14.0% as legal professionals and 8.9% as technology experts or educators.[34] The sample was gathered through convenience and snowball circulation rather than random probability sampling, skews toward younger, urban and more educated respondents than the Indian population at large and the role-specific sub-samples are small (parents, n = 37; legal professionals, n = 22; technologists, n = 14); the findings below are accordingly read as indicative of attitudes within an educated, digitally engaged cross-section of Indian society, not as a statistically representative account of the national population and no inferential statistical tests were run given the sample size and sampling method. Three questions were asked of all 157 respondents regardless of role. Support for a law limiting a child's digital freedom in exchange for guaranteed safety was strong: the mean response on a five-point agreement scale was 3.97, with 68.2% selecting agree or strongly agree.[35] Asked who should be the primary protector; of a child online, respondents placed the greatest weight on parents (42.7%), followed by technology companies (23.6%), the State (19.1%) and the child's own capacity for self-regulation (14.6%).[36]And an emphatic 84.1% described the DPDP Act, 2023 overall as a step forward for digital freedom, against 11.5% who called it a step backward.[37]

The role-specific branches surface sharper findings. Among the 37 respondents identifying as parents, only 48.6% were aware that the DPDP Act gives them a legal right to demand deletion of their child's data,[38] 75.7% rated their trust in major social media platforms to protect their child at 1 or 2 out of 5,[39] and faced with a hypothetical Aadhaar-based age-verification request, 45.9% said they would

[30] Digital Personal Data Protection Rules, 2025, G.S.R. 700(E), 13 November 2025, r 10.
[31] DPDP Rules, 2025 (n 22), r 11 and Fourth Schedule.
[32] Author's primary survey data, "The Privacy-Safety Paradox: Reconciling Child Rights in Digital India"(2026), N = 157. Raw response data on file with the author.
[33] Author's survey data (n 23), demographic responses: Age Group and Educational Qualification fields.
[34] Author's survey data (n 23), Primary Role field.
[35] Author's survey data (n 23), item: I support a law that limits a child's digital freedom if it guarantees their online safety, n = 157, mean = 3.97, 4-5 response rate = 68.2%.
[36] Author's survey data (n 23), item: Who do you believe should be the 'Primary Protector' of a child's safety and privacy online?, n = 157.
[37] Author's survey data (n 23), item: Overall, do you believe India's DPDP Act 2023 is a step forward or a step backward for 'Digital Freedom'?, n = 150 (7 non-responses).
[38] Author's survey data (n 23), item: Are you aware that the Indian DPDP Act 2023 gives you the legal right to ask companies to delete your child's data?, n = 37.
[39] Author's survey data (n 23), item: Rate your trust in Social Media companies, to protect your child from strangers, n = 37.

delete the app rather than comply.[40] Among the 22 legal professionals surveyed, opinion on the DPDP Act's balance was almost evenly split: 50.0% considered it insufficiently protective of child safety, against 45.5% who considered it well-balanced.[41] Among the 14 technologists and educators surveyed, 71.4% rated the Section 9(3) prohibition on behavioral tracking as necessary to protect a child's Article 21 right to privacy.[42]

The most striking finding however, comes from the 84 respondents who answered as students reflecting on their own digital adolescence. 53.6% admitted having lied about their age to join a social media platform while still a minor[43] and 51.2% admitted having used a VPN, incognito mode or a secondary "private" account specifically to bypass parental or age-based restrictions.[44] These are self-reported recollections rather than platform audit data and should be read with that caveat but they offer direct first-person evidence that an age-verification architecture built on a self-declared birth date is only as reliable as a minor's incentive to be truthful about it an incentive that on this evidence is frequently absent.

These limitations are disclosed in the interest of academic transparency: a non-probability, youth and education-skewed sample of this size cannot support population-level claims about India as a whole and the small role-specific sub-samples preclude confident sub-group comparison.

X Comparative Legal Analysis

10.1 United States: Children's Online Privacy Protection Act (COPPA)

COPPA applies to children under thirteen years and is enforced by the Federal Trade Commission which has issued detailed guidance on acceptable methods of obtaining verifiable parental consent including signed forms, credit-card verification and video-conferencing confirmation. COPPA's narrower age threshold relative to the DPDP Act's eighteen-year cut-off reflects a policy choice to regulate more intensively a smaller more clearly vulnerable cohort, while relying on general consumer-protection law for older minors.

10.2 United Kingdom: The Age-Appropriate Design Code

The UK Information Commissioner's Office's statutory code of practice requires online services likely to be accessed by children to apply a 'best interests of the child' standard high privacy settings by default and data-minimization principles calibrated across defined age bands rather than a single threshold. This risk-tiered design offers a potential model for India where a single eighteen-year threshold currently applies uniformly regardless of a minor's actual developmental stage or digital literacy.

10.3 European Union: GDPR, Article 8

The GDPR permits Member States to set the age of consent for information-society services between thirteen and sixteen years below which parental consent is required. This flexibility acknowledges variation in national child-development and digital-literacy assumptions in contrast to the DPDP Act's fixed eighteen-year threshold.

10.4 Australia: Online Safety Act, 2021

Australia's Online Safety Act establishes a dedicated eSafety Commissioner with statutory powers to order removal of cyberbullying material, image-based abuse content and CSAM, operating alongside Australia's separate privacy law. This model of a specialized child-online-safety regulator, distinct from the general data-protection authority, contrasts with India's current approach of housing children's data protection within the general-purpose Data Protection Board.

10.5 Comparative Insights for India

The comparative survey suggests three design

[40] Author's survey data (n 23), item: If an app requires your child's Aadhaar for 'Age Verification,' would you allow it or delete the app?, n = 37.
[41] Author's survey data (n 23), item: In your professional opinion, does the DPDP Act 2023 strike a fair balance between Child Safety and Digital Privacy?, n = 22.
[42] Author's survey data (n 23), item: The prohibition of 'Behavioral Tracking'
[43] Author's survey data (n 23), item: When you were younger, did you ever lie about your age..., n = 84.
[44] Author's survey data (n 23), item: Did you ever use VPNs, Incognito mode, or secondary 'private' accounts... to bypass parental or age-based restrictions?, n = 84.

choices meriting consideration: age-tiered rather than binary consent thresholds; statutory technical standards for age-verification methods rather than an open-ended 'verifiable consent' obligation; and either a dedicated child-online-safety function or formal statutorily mandated coordination between the Data Protection Board and existing child-protection authorities such as the NCPCR.

XI. Critical Analysis: Fragmentation Across Four Regimes

First, jurisdictional and institutional fragmentation. POCSO offences are investigated by state police and prosecuted before Special Courts under the Ministry of Home Affairs' broader criminal justice architecture; IT Act intermediary obligations are administered by the Ministry of Electronics and Information Technology; and the DPDP Act creates an entirely new body, the Data Protection Board of India whose powers over child-data violations only become operative once the Rules' staggered commencement schedule runs its course.[45] A platform that hosts CSEAM and simultaneously profiles a child's behavioral data commercially could in principle face proceedings before three separate authorities operating under three separate statutes with no formal mechanism for coordinated referral.

Second, definitional inconsistency. POCSO and the IT Act define a child consistently as anyone under eighteen and the DPDP Act adopts the identical threshold[46] a point of genuine coherence across the criminal and data-protection regimes. Where the frameworks diverge is in the precision of their operative definitions: POCSO's 2019 amendment gave "child pornography" (now CSEAM) a detailed statutory definition and Section 67B similarly defines "sexually explicit act," yet the DPDP Rules leave "reliable details" for parental verification wholly undefined resting on a single illustrative example rather than a tested standard.[47] A framework this precise about the harm it criminalizes ought to be at least as precise about the safeguard it mandates.

Third, the absence of a data-linked reporting bridge. Section 21 of POCSO and the 2021 Intermediary Guidelines both impose reporting obligations when CSEAM is discovered[48] but neither instrument requires a platform to report to the Data Protection Board when the same investigation reveals unlawful profiling or non-consensual data collection involving the same child. The 2024 *S. Harish* ruling closed the gap between POCSO and the IT Act; no equivalent judicial or statutory bridge yet exists between either of those regimes and the DPDP Act.

Fourth, encryption and platform design tensions. The obligation on significant social media intermediaries to proactively identify CSEAM sits uneasily beside the widespread use of end-to-end encryption on messaging platforms, a tension repeatedly flagged in commentary on Section 67B enforcement.[49] The DPDP Act's child-data provisions add a further design constraint platforms must now also build age-verification and consent-capture infrastructure without any coordinated technical standard connecting the two design obligations leaving platforms to build parallel uncoordinated compliance systems for what is from the child's perspective, a single relationship of trust.

XII Critical Gaps and Challenges

12.1 Definitional and Threshold Inconsistency

Although POCSO, the JJ Act and the DPDP Act each define a 'child' as a person below eighteen years, the practical consequences of this common threshold diverge sharply: POCSO applies with equal criminal force regardless of a child's age within that band whereas the DPDP Act applies a uniform consent requirement to a sixteen-year-old digitally literate teenager and a five-year-old child

[45] DPDP Rules, 2025 (n 22); commencement staggered with the substantive child-data provisions taking effect 13 May 2027, per the Ministry's Enforcement Notification dated 13 November 2025.
[46] POCSO Act (n 1), s 2(1)(d); IT Act (n 4) read with POCSO for CSAM purposes; DPDP Act (n 5), s 2(f).
[47] Draft Digital Personal Data Protection Rules, 2025, illustration to r 10 (retained in substance in the final Rules); see critique in Chambers and Partners (n 9).
[48] POCSO Act (n 1), s 21; Intermediary Guidelines and Digital Media Ethics Code Rules, 2021.
[49] See discussion of encryption-related enforcement challenges in ApniLaw (n 12) and Disaster.Shiksha, "Child Sexual Abuse Material Online: Section 67B IT Act and the Janhit Manch PIL" (2026).

alike without the age-tiering found in comparable foreign frameworks.

12.2 The Verification Paradox

Verifiable parental consent presupposes reliable mechanisms to establish both a user's status as a minor and the identity authority of the consenting parent. India's principal digital-identity instrument, Aadhaar was not designed for and is not typically deployed in routine consumer age-verification and mandating its use for this purpose would risk compounding the very informational-privacy harm the DPDP Act seeks to prevent by requiring platforms to collect additional sensitive identity data from families. The DPDP Rules, 2025 do not yet prescribe a standardized and privacy-preserving technical method for age assurance leaving compliance largely to self-certification by platforms.

12.3 Institutional and Enforcement Fragmentation

A child harmed through online data practices that culminate in grooming or abuse may need to engage, simultaneously or sequentially with the Data Protection Board of India (for the data-protection violation), a Special POCSO Court (for the sexual offence) the police cybercrime cell (for offences under the IT Act) and the NCPCR or Child Welfare Committee (for welfare and rehabilitation). No statutory mechanism currently requires these bodies to share information or coordinate proceedings creating the risk that a single continuum of harm is treated as unrelated siloed complaints.

12.4 The Phased Implementation Gap

Because significant DPDP Rules provisions - including those governing consent managers and the Data Protection Board's full adjudicatory powers - do not take effect until November 2026 and May 2027 respectively, children remain, for a transitional period of several years, formally protected by statute but without a fully operative enforcement mechanism.

12.5 Deterrence and Penalty Design

The DPDP Act's tiered financial penalties reaching up to ₹200 crore for violations concerning children's data are calibrated primarily with large data fiduciaries in mind. Their deterrent effect on small and mid-sized educational-technology and gaming platforms - which collect substantial volumes of children's data but operate with limited compliance budgets - remains untested and warrants closer regulatory and scholarly attention.

XIII. Conclusion and Suggestions

India's protective framework for children in digital spaces is, on balance, more comprehensive today than at any earlier point: POCSO criminalizes the underlying abuse, the IT Act and the 2021 Rules bind the platforms that carry it, *S. Harish* forged a working link between the two, *Puttaswamy* supplied the constitutional foundation for treating a child's data as deserving of protection in its own right and the DPDP Act finally gives that foundation statutory teeth. What the framework still lacks is a formal mechanism for treating these four regimes as expressions of a single underlying commitment rather than as separate silos administered by separate ministries under separate timelines.

- **A coordinated referral protocol** between the Special Courts constituted under POCSO, the nodal cyber-crime authorities administering the IT Rules and the Data Protection Board of India, so that a single investigation touching both CSEAM and unlawful child-data processing need not proceed as three unconnected matters.
- Harmonize the definitional and procedural treatment of 'child' across POCSO, the JJ Act and the DPDP Act which introduce age-tiered obligations under the DPDP Rules analogous to the UK Age-Appropriate Design Code.
- **A defined, tested standard for "reliable details"** under Rule 10 of the DPDP Rules, published as subordinate technical guidance before the child-data provisions commence in May 2027, matching the definitional precision POCSO and Section 67B already apply to the harms they criminalize.
- A public-awareness campaign targeted at parents, given the survey finding that fewer than half of surveyed parents know they can demand deletion of their child's data as a right that exists on the statute book but has not yet reached the people meant to exercise it.
- Accelerate, where administratively feasible, the phased implementation timeline for child-

specific provisions of the DPDP Rules, given the urgency of the harms involved, rather than deferring them to the general 1288-1299 schedule applicable to all data fiduciaries.

- Calibrate penalty and compliance-support structures to distinguish between large data fiduciaries and small or early-stage ed-tech and gaming platforms, to ensure deterrence without disproportionately burdening smaller compliant actors.
- Prescribe standardised, privacy-preserving technical methods for age assurance and verifiable parental consent under the DPDP Rules, rather than leaving the standard open-ended.
- **Alignment of DPDP Board timelines with existing child-protection enforcement**, so that the 2027 commencement of child-data obligations does not leave a multi-year gap during which POCSO and IT Act enforcement continue without any parallel data-protection oversight of the same platforms.

Until such coordination exists on the statute books rather than merely in judicial obiter or survey commentary India's protection of children online will remain what this paper has described: four strong but separately maintained walls, each broadly welcomed by the public it serves but not yet joined into a single connected structure.

References

Protection of Children from Sexual Offences Act, 2012 (India).

Protection of Children from Sexual Offences (Amendment) Act, 2019 (India).

Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008 (India).

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

Juvenile Justice (Care and Protection of Children) Act, 2015 (India).

Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 (India).

Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology, 13 November 2025 (India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

Children's Online Privacy Protection Act, 15 U.S.C. 1288-1299 (1998) (United States).

Information Commissioner's Office (UK), Age-Appropriate Design Code: A Code of Practice for Online Services.

Regulation (EU) 2016/679 (General Data Protection Regulation), Article 8.

Online Safety Act 2021 (Commonwealth of Australia).