THE VERIFICATION PARADOX: A SOCIO-LEGAL CRITIQUE OF VERIFIABLE PARENTAL CONSENT UNDER INDIA'S DPDP FRAMEWORK

Shweta Chaturvedi, Solace Law Practice

ABSTRACT

This article interrogates the requirement of verifiable parental consent (VPC) under Section 9 of India's Digital Personal Data Protection Act, 2023 through a socio-legal and constitutional lens. It argues that the Act's identity-centric design produces a "verification paradox," whereby mechanisms intended to protect children incentivise excessive data collection, erode privacy, and undermine adolescent autonomy. By mandating uniform parental consent for all individuals below eighteen, the framework adopts a structurally overbroad approach that conflicts with constitutional proportionality, ignores the principle of evolving capacities, and departs from comparative global standards. The article further demonstrates how the operationalisation of VPC under the DPDP Rules, 2025 generates systemic incentives toward identity-heavy compliance practices, contradicting the Act's own commitments to data minimisation and purpose limitation. It critiques the discretionary exemption regime under Section 9(4) as administratively unstructured and normatively vulnerable to arbitrariness and market capture. Situating the analysis within India's broader political economy of digital governance and drawing parallels with Aadhaar's function creep, the article highlights the exclusionary consequences of VPC for marginalised children and adolescents. It concludes by advancing a reform-oriented framework grounded in proportionality, privacy-preserving age assurance, differentiated age thresholds, and constitutionally coherent regulatory design.

I. Regulatory Architecture and the Logic of Verification

India's Digital Personal Data Protection (DPDP) Act, 2023 represents a serious legislative attempt to mediate the increasingly fraught relationship between individual privacy and the infrastructural demands of a rapidly expanding digital economy. Enacted in the aftermath of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the statute carries the constitutional weight of operationalising informational privacy as a fundamental right rather than merely a policy aspiration.[1] Yet within this framework, Section 9, which governs the processing of children's data, reveals a deeper regulatory anxiety. Through its insistence on verifiable parental consent (VPC) for all individuals below eighteen years of age, the provision exemplifies a broader tendency in Indian digital governance: the belief that protection is best achieved through intensified verification and identity-based control.[2] This article argues that such an approach produces a "verification paradox", wherein mechanisms designed to protect minors from harm inadvertently undermine privacy, autonomy, and equality, while simultaneously contradicting the DPDP Act's own normative commitments to data minimisation and proportionality.[3]

Section 9(1) mandates that data fiduciaries obtain verifiable consent from a parent or lawful guardian prior to processing the personal data of any child, defined expansively as any person below eighteen years.[4] The DPDP Rules, 2025, particularly Rule 10, operationalise this obligation by requiring fiduciaries to implement technical and organisational measures capable of reliably verifying both the age of the user and the authenticity of the parental relationship.[5] Although neither the Act nor the Rules explicitly mandate the use of Aadhaar or other state-issued identifiers, the regulatory expectation of "robust" and "verifiable" consent has, in practice, created strong incentives for platforms to adopt high-assurance identity mechanisms such as government-issued IDs, DigiLocker credentials, or Aadhaar-based authentication.[6] The structure of compliance thus quietly normalises identity-intensive verification as the default

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[2] Digital Personal Data Protection Act, No. 22 of 2023, § 9 (India).
[3] Taxmann, Digital Guardianship: A Comprehensive Analysis of Children's Digital Data Protection Under India's DPDP Act 2023, https://www.taxmann.com/research/company-and-sebi/top-story/105010000000027105/digital-guardianship-a-comprehensive-analysis-of-childrens-digital-data-protection-under-indias-dpdp-act-2023-experts-opinion.
[4] Digital Personal Data Protection Act § 9(1).
[5] Digital Personal Data Protection Rules, 2025, r. 10 (India).
[6] Vision IAS, DPDP Rules 2025: Framework for Personal Data Protection (Nov. 14, 2025), https://www.visionias.in/blog/current-affairs/dpdp-rules-2025-framework-for-personal-data-protection.

pathway to legal conformity.

This design choice is not trivial. It reshapes the entire logic of child protection within digital environments. The prohibition on behavioural monitoring, tracking, and targeted advertising directed at minors, as well as the restriction on processing likely to cause "detrimental effect" to a child's well-being, reflects a legitimate concern with exploitative practices across sectors such as EdTech, gaming, and social media.[7] Yet the architecture of Section 9 does not distinguish between contexts of high and low risk, nor between early childhood and late adolescence. A seventeen-year-old seeking access to peer-support platforms, reproductive health information, or anonymous mental health resources is subjected to the same regulatory structure as a young child accessing entertainment content. This flattening of developmental capacity effectively erases the concept of evolving autonomy, a principle long recognised in child rights discourse and increasingly reflected in comparative data protection regimes.[8]

II. Proportionality, Overbreadth, and Constitutional Incoherence

The constitutional implications of this approach become clearer when analysed through the proportionality doctrine articulated in *Puttaswamy*. The four-pronged test of legality, legitimate aim, necessity, and proportionality stricto sensu demands that any restriction on fundamental rights must be narrowly tailored and represent the least restrictive means available.[9] While Section 9 satisfies the first two prongs, the difficulties emerge sharply at the third and fourth stages. The requirement of parental consent in all cases, regardless of the nature of the service, the maturity of the user, or the risk profile of the processing, results in a measure that is structurally overbroad.[10]

Indian constitutional jurisprudence has consistently emphasised that overinclusive measures are constitutionally suspect. In *Modern Dental College & Research Centre v. State of Madhya Pradesh*, the Court clarified that a restriction which sweeps more broadly than necessary fails

[7] CUTS CCIER, Economic Analysis of Verifiable Parental Consent Mechanisms (2025), https://cuts-ccier.org/pdf/economic-analysis-of-verifiable-parental-consent-mechanisms-evaluating-impact-on-consumers-and-data-fiduciaries.pdf.

[8] NUJS Intellectual Property & Technology Law Society, Verifiable Parental Consent and Age Verification (Mar. 19, 2025), https://nujsiplaw.wordpress.com/2025/03/19/verifiable-parental-consent-and-age-verification-a-comparative-analysis-of-indias-draft-digital-personal-data-protection-rules-and-childrens-online-privacy-protection-act/.

[9] Puttaswamy, supra note 1.

[10] Law School Policy Review, The Curious Case of Common Consent (Dec. 4, 2025), https://lawschoolpolicyreview.com/2025/12/04/the-curious-case-of-common-consent-rethinking-verifiable-parental-consent-under-the-dpdpa-2023/.

the necessity requirement even if its objective is legitimate.[11] Similarly, in *Anuradha Bhasin v. Union of India*, the Court insisted that restrictions affecting fundamental rights must be temporally, territorially, and substantively proportionate.[12] Applied to Section 9, the absence of any internal differentiation within the category of "children" appears constitutionally indefensible. A regulatory framework that deters adolescents from accessing essential information or expressing themselves freely online cannot plausibly be described as the least restrictive means of achieving child protection.[13]

Comparative regimes underscore the excessiveness of India's approach. Under the EU's General Data Protection Regulation, Article 8 sets the default age of digital consent at thirteen, while permitting Member States to raise the threshold to a maximum of sixteen.[14] The US Children's Online Privacy Protection Act (COPPA) similarly restricts its application to children below thirteen.[15] Empirical studies of COPPA's operation suggest that stringent parental consent requirements often lead platforms to exclude minors entirely or to encourage misrepresentation of age, thereby undermining both protection and participation.[16] Against this background, India's blanket eighteen-year threshold appears not as a carefully calibrated safeguard but as a maximalist response unmoored from evidence-based regulation.

Beyond proportionality, the VPC framework introduces a deeper doctrinal incoherence within the DPDP Act itself. Section 5 codifies principles of data minimisation and purpose limitation, positioning them as foundational obligations for all data fiduciaries.[17] Yet the practical effect of Rule 10 is to incentivise exactly the opposite behaviour. To demonstrate compliance, fiduciaries are encouraged to collect government-issued identifiers, establish relational databases linking parent and child, and retain verification records over extended periods.[18] The result is the gradual construction of family-linked identity infrastructures fundamentally incompatible with the principle of minimisation.

[11] Modern Dental Coll. & Rsch. Ctr. v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
[12] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
[13] NUALS Law Journal, Age Checks or Privacy Wrecks? (Aug. 7, 2025), https://nualslawjournal.com/2025/08/07/age-checks-or-privacy-wrecks-decoding-rule-10-of-dpdp-draft-rules-2025/.
[14] Regulation (EU) 2016/679, art. 8, 2016 O.J. (L 119) 1.
[15] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.
[16] New America, Exploring Privacy-Preserving Age Verification (July 16, 2025), http://newamerica.org/oti/briefs/exploring-privacy-preserving-age-verification/.
[17] Digital Personal Data Protection Act § 5.
[18] NUALS Law Journal, supra note 13.

This contradiction reflects a broader pattern in Indian digital governance. The trajectory of Aadhaar offers a cautionary parallel. Originally conceived as a targeted welfare delivery mechanism, Aadhaar gradually expanded into a near-universal identification infrastructure, enabling widespread authentication across public and private domains. Scholars have documented how this expansion facilitated function creep and increased surveillance capacity despite judicial attempts to impose doctrinal limits.[19] The VPC regime risks replicating this pattern in the private sector, where platforms, in an effort to demonstrate compliance, may accumulate sensitive relational data far beyond what is necessary for child protection. Reports of vulnerabilities and systemic risks in child-data ecosystems within EdTech further underscore that these risks are not speculative.[20]

III. Discretion, Exclusion, and the Political Economy of VPC

The exemption mechanism under Section 9(4) further complicates the regulatory landscape. By authorising the Central Government to exempt certain data fiduciaries from VPC obligations if they are deemed "verifiably safe," the provision introduces a discretionary carve-out that is entirely undefined within the statute. No criteria are articulated, no procedural safeguards are specified, and no transparency obligations are imposed. This absence of structure raises classical concerns under Indian administrative law regarding arbitrary discretion and excessive delegation. In *A.K. Kraipak v. Union of India*, the Supreme Court emphasised that unfettered discretion is inherently antithetical to the rule of law.[21] The likely outcome of Section 9(4) is regulatory asymmetry: dominant market actors with institutional access may secure exemptions, while smaller platforms bear the full burden of compliance. Such a regime risks entrenching market power while simultaneously eroding the legitimacy of the regulatory framework.[22]

The socio-economic consequences of VPC further complicate its normative justification. India's digital divide is not merely infrastructural but deeply social. A significant proportion of households lack stable access to formal identification, reliable authentication mechanisms, or digital literacy. For such populations, VPC does not operate as a protective mechanism but

[19] Usha Ramanathan, A Unique Identity Bill, 2010: Concerns and Questions, 45 ECON. & POL. WKLY. 30 (2010).
[20] DSCI, Summary – DPDP Rules 2025, https://www.dsci.in/files/content/documents/2025/Digital-Personal-Data-Protection-Rules-2025.pdf.
[21] A.K. Kraipak v. Union of India, (1969) 2 SCC 262 (India).
[22] Law.asia, Indian Perspective on Protecting Children's Personal Data Under DPDP Act (May 8, 2025), https://law.asia/childrens-data-protection-dpdp-act/.

as a barrier to participation. Children from marginalised communities risk being systematically excluded from educational platforms, health services, and civic spaces increasingly mediated through digital systems.[23] This exclusion has direct implications for the right to education under Article 21A and the guarantee of equality under Article 14.[24] The impact is particularly acute for adolescent girls, whose access to information relating to sexual and reproductive health may already be constrained by social norms. Mandatory parental verification in such contexts can function less as protection and more as surveillance, reinforcing existing power asymmetries within households.[25]

Crucially, these outcomes are not inevitable. They are the result of design choices. Alternative regulatory architectures already exist and are being actively developed in other jurisdictions. Privacy-preserving age assurance mechanisms, such as zero-knowledge proofs, enable verification of eligibility without disclosure of underlying identity.[26] Consent managers recognised under Section 13 of the DPDP Act could be leveraged as intermediaries that issue anonymised attestations rather than transmitting raw personal data.[27] Tokenised verification models within India Stack further demonstrate that high-assurance authentication need not rely on biometric exposure.[28] Comparative developments in jurisdictions such as the UK and Australia illustrate that it is possible to design child-protection regimes that prioritise proportionality and minimisation without collapsing into identity-centric governance.[26]

The persistence of identity-centric regulation in India thus reflects not technological constraint but regulatory imagination. Section 9 embodies a broader anxiety within Indian governance: a preference for legibility, control, and verification over autonomy, trust, and decentralisation. The verification paradox emerges precisely because protection is conceptualised through the lens of identification. The more the state seeks to protect children by mandating verification, the more it incentivises the accumulation of sensitive data, the construction of surveillance infrastructures, and the exclusion of vulnerable populations.[27]

A more constitutionally coherent approach would require significant recalibration. Differentiated age thresholds sensitive to adolescent autonomy, risk-based application of VPC

[23] Drishti IAS, DPDP Act 2023 and DPDP Rules 2025, https://www.drishtiias.com/daily-updates/daily-news-analysis/dpdp-act-2023-and-dpdp-rules-2025.
[24] INDIA CONST. arts. 14, 21A.
[25] Assurtiv, Child Data Protection Rules 2025 Under DPDP Act, https://assurtiv.com/child-data-protection-rules-2025-under-dpdp-act/.
[26] New America, supra note 16.
[27] Digital Personal Data Protection Act § 13.

obligations, statutory recognition of privacy-preserving verification mechanisms, and structured constraints on executive discretion are not merely policy preferences but constitutional necessities.[28] Without such reforms, Section 9 risks becoming emblematic of a deeper failure within India's data protection project: the inability to reconcile technological governance with constitutional fidelity.

Child protection in the digital age cannot be achieved through the proliferation of identity systems alone. It requires a commitment to privacy by design, sensitivity to social context, and fidelity to constitutional principle. Until Section 9 is reimagined along these lines, the DPDP framework will remain haunted by its own paradox: a law designed to protect children that ultimately undermines their autonomy, access, and dignity in the very spaces it seeks to regulate.[29]

[28] DPO Club, Decoding the Nuances of Verifiable Parental Consent Under the DPDPA (Dec. 21, 2025), https://dpoclub.in/blog/decoding-the-nuances-of-verifiable-parental-consent-under-the-dpdpa.
[29] IJFMR, A Comparative Analysis of Data Protection Laws in India, UK, and USA (2025), https://www.ijfmr.com/papers/2025/3/45887.pdf.