GUARDIAN IN THE CODE: CRITICAL ANALYSIS OF CHILDREN'S DATA PROTECTION UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND RULES, 2025

Parastish Dubey, Amity University, Lucknow

Dr. Reshma Umair, Amity University, Lucknow

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDPA) and the Digital Personal Data Protection Rules, 2025 (DPDP Rules) together constitute India's first comprehensive legislative framework for personal data protection. Section 9 of the DPDPA occupies a position of singular importance within this framework — it establishes a specialized regime for the protection of children's personal data, predicated on three pillars: verifiable parental consent, an absolute prohibition on tracking and behavioural monitoring, and a categorical ban on targeted advertising directed at minors. This paper critically analyses the architecture of Section 9, the operationalising provisions under Rules 10–12 and the Fourth Schedule, and the practical and doctrinal lacunae that persist even after the finalization of the Rules. Drawing on comparative frameworks including the EU's General Data Protection Regulation (GDPR), the United States' Children's Online Privacy Protection Act (COPPA), and the UK Age Appropriate Design Code (AADC), this paper argues that while Section 9 represents a paradigm shift in India's approach to child digital rights, significant gaps remain — particularly around age verification infrastructure, enforcement capacity, and the tension between child protection and data minimization. The paper concludes with recommendations for bridging these gaps in the implementation phase.

Keywords: DPDPA 2023, DPDP Rules 2025, Children's Data Protection, Verifiable Parental Consent, Section 9, Data Fiduciary, Behavioural Tracking, GDPR, COPPA, Digital Child Rights.

I. INTRODUCTION

India is home to over 560 million internet users, a substantial proportion of whom are minors. Children engage daily with social media platforms, educational applications, gaming portals, and e-commerce services — generating vast quantities of personal data in the process. Until the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA), India lacked a dedicated statutory framework to govern this data. The existing regime under the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 was widely regarded as inadequate, offering no specific protections for minors.

The enactment of the DPDPA marked a decisive break from this inadequacy. Enacted on August 11, 2023, the Act establishes a consent-driven, rights-based framework for personal data governance. The Digital Personal Data Protection Rules, 2025, notified on November 14, 2025 by the Ministry of Electronics and Information Technology (MeitY), operationalize the Act's mandates — including those specific to children — and inaugurated a phased implementation timeline culminating in full enforcement by May 2027.

Section 9 of the DPDPA, read with Rules 10–12 of the DPDP Rules, 2025, constitutes the first child-specific data protection framework in Indian statutory law. Its enactment is significant not merely as a regulatory milestone but as a statement of constitutional principle: that the privacy of children in digital spaces is a matter of fundamental rights, not mere policy preference. The Supreme Court of India, in Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, recognized the right to privacy as a fundamental right under Article 21 of the Constitution, with particular resonance for informational privacy. Section 9 translates this constitutional commitment into specific obligations for data fiduciaries.

This paper proceeds in five parts. Part II surveys the pre-DPDPA legal landscape for children's data in India. Part III provides a detailed doctrinal analysis of Section 9 and Rules 10–12. Part IV offers a comparative analysis with the GDPR, COPPA, and UK AADC. Part V identifies persistent gaps and doctrinal challenges. Part VI offers concluding observations and recommendations.

II. THE PRE-DPDPA LANDSCAPE: AN ABSENCE OF PROTECTION

Prior to the DPDPA, no Indian statute directly addressed the collection, processing, or

use of personal data belonging to children in digital spaces. The Information Technology Act, 2000 (IT Act), while creating a broad framework for electronic governance and cybercrime, made no meaningful distinction between adult and child data subjects. The SPDI Rules, 2011 introduced the concept of 'sensitive personal data or information' but did not carve out a protective category for minors.

The Protection of Children from Sexual Offences Act, 2012 (POCSO) and the Juvenile Justice (Care and Protection of Children) Act, 2015 addressed offline child protection and certain digital harms respectively, but neither governed data collection practices by platforms. In practice, platforms operating in India routinely set their minimum age at 13 (mirroring COPPA's US standard) without any statutory basis for doing so, and without any mechanism to verify user age or obtain parental authorization.

Judicial intervention filled part of this vacuum. Courts recognized, in cases including Shreya Singhal v. Union of India, (2015) 5 SCC 1, the constitutional dimensions of digital speech and privacy. However, no court delivered a comprehensive ruling on children's data rights specifically. The result was an enforcement landscape marked by ad hoc decision-making and platform self-regulation, which proved manifestly insufficient as child exposure to online harms — including targeted advertising, data profiling, and cyber grooming — escalated sharply.

A 2021 report cited by researchers noted a 261% rise in cybercrime against children in India, with cyber pornography and grooming among the leading offences. The COVID-19 pandemic accelerated the migration of children into digital environments, exposing them to data-driven harms at unprecedented scale. This context renders the legislative intervention effected by Section 9 not merely timely but overdue.

III. STATUTORY ANALYSIS: SECTION 9 AND DPDP RULES, 2025

A. Definitional Framework

Section 2(k) of the DPDPA defines a 'child' as 'an individual who has not completed the age of eighteen years.' This is a bright-line rule admitting of no sub-categories or graduated treatment based on maturity or context. By contrast, the GDPR provides Member States the discretion to lower the age threshold to 13 for information society services (Article 8(1)). The

DPDPA's uniform 18-year threshold reflects a deliberate legislative choice to afford maximum protection, although as discussed in Part V, this creates significant practical challenges for platforms.

Notably, Section 9 also extends its protections to 'a person with disability who has a lawful guardian,' recognizing that vulnerability to data exploitation is not confined to chronological age. This parallel treatment of children and persons with disabilities within a single provision signals a broader conception of protected persons that is both progressive and constitutionally resonant.

B. The Verifiable Parental Consent Requirement

Section 9(1) imposes a mandatory requirement that a data fiduciary obtain 'verifiable consent of the parent of such child or the lawful guardian' before processing any personal data of a child. The word 'verifiable' is critical. It transforms consent from a formality — such as a user clicking 'I agree' — into a substantive obligation requiring positive confirmation of parental identity and authorization.

Rule 10 of the DPDP Rules, 2025 operationalizes this requirement. It mandates that data fiduciaries first ascertain whether the user seeking access to their service is a child, then validate the identity and age of the child's parent or guardian, and finally obtain a verifiable, traceable consent from that parent before processing commences. Importantly, Rule 10 states that this obligation is in addition to the general consent requirements under Section 6 of the Act and Rule 3 of the Rules.

Rule 10 also contemplates a Common Consent Mechanism (CCM), allowing multiple service providers to rely on a single shared platform — potentially an app store or a government-authorized intermediary — for the purposes of obtaining verifiable parental consent. This represents a pragmatic acknowledgment of the scalability problem inherent in requiring every individual data fiduciary to independently operate a consent verification system.

C. Absolute Prohibitions: The Triple Lock

Section 9(3) imposes three absolute prohibitions on data fiduciaries processing children's data: (i) tracking or behavioural monitoring of children; (ii) targeted advertising

directed at children; and (iii) any form of processing likely to cause detrimental effects on the well-being of a child. These prohibitions operate as a 'triple lock' — they cannot be waived even with parental consent, distinguishing them from the consent-based obligations under Section 9(1).

The behavioural monitoring prohibition is particularly significant given the centrality of data profiling to the business models of social media platforms, educational technology companies, and gaming services. Following a child across websites, building a behavioural profile from app usage data, or inferring personality traits from content interaction patterns — all such activities are categorically barred under the DPDPA regime.

Section 9(2) independently prohibits processing that is 'likely to cause any detrimental effect on the well-being of a child.' This is a broad, effects-based standard with no exhaustive definition provided in the Act or Rules. Its interpretation will likely evolve through Data Protection Board (DPB) adjudication and potentially through litigation before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which serves as the appellate authority under the Act.

D. Exemptions: Rules 11–12 and the Fourth Schedule

Section 9(4) permits the Central Government to exempt certain classes of data fiduciaries from the consent and monitoring obligations, subject to conditions. Rules 11–12 and the Fourth Schedule to the DPDP Rules give effect to this power by establishing two categories of exemption.

Part A of the Fourth Schedule exempts certain data fiduciaries entirely from the parental consent requirement, provided they restrict processing to specified purposes. These include clinical establishments and mental health providers (for health service delivery), educational institutions (for educational purposes), and child transport operators. Part B of the Schedule exempts processing conducted for the exercise of powers or fulfilment of duties under any law in force in India in the interest of the child, as well as processing for the provision of subsidies, benefits, and services falling within 'legitimate use' under Section 7(b) of the Act.

These exemptions are narrowly tailored — they apply only to the extent necessary for the specified purpose and do not release fiduciaries from other obligations under the Act such

as data breach notification, grievance redressal, and the general prohibition on detrimental processing under Section 9(2).

Section 9(5) provides a further mechanism: the Central Government may, upon satisfaction that a data fiduciary processes children's data in a 'verifiably safe' manner, notify a lower age threshold applicable to that specific fiduciary. This creates a positive incentive mechanism — platforms that invest in child-safe data practices may be rewarded with reduced regulatory burden for older adolescents.

E. Penalties

Non-compliance with the obligations under Section 9 attracts penalties of up to Rs. 200 crore under the DPDP Act. This is the second highest penalty tier under the Act, reflecting the legislature's prioritization of children's data protection. The highest tier — Rs. 250 crore — applies to failures to maintain reasonable security safeguards resulting in a data breach.

IV. COMPARATIVE ANALYSIS

A. GDPR (European Union)

Article 8 of the GDPR establishes the legal framework for processing personal data of children in relation to information society services. While the GDPR sets 16 as the default consent age, it grants Member States the discretion to lower this to 13. This graduated approach reflects the principle of evolving capacities — a recognition, drawn from international child rights law, that children's ability to exercise autonomous rights increases with age and maturity.

The GDPR also mandates that controllers make reasonable efforts to verify parental consent, having regard to available technology. However, it does not prescribe a specific verification mechanism, leaving implementation to sector-specific guidance and supervisory authority decisions. The UK Age Appropriate Design Code (Children's Code), while strictly speaking post-Brexit, offers the most sophisticated child data protection regime globally — imposing fifteen standards including data minimization by default, profiling off by default, and geolocation off by default for child users, regardless of consent.

India's DPDPA compares favourably with the GDPR on the age threshold, maintaining the uniform 18-year standard without the dilution permitted by GDPR. However, the DPDPA

currently lacks the GDPR's accountability tools such as Data Protection Impact Assessments (DPIAs) specifically mandated for child data processing, though Significant Data Fiduciaries are required to conduct annual DPIAs under Rule 13 of the DPDP Rules.

B. COPPA (United States)

The Children's Online Privacy Protection Act, 1998 (COPPA) applies to operators of websites or online services directed at children under the age of 13, and to those who knowingly collect personal information from children. COPPA requires clear privacy notices, verifiable parental consent before data collection, and parental rights of access and deletion.

The Federal Trade Commission (FTC) has acknowledged the Common Consent Mechanism in its implementation guidance — a framework analogous to the CCM introduced under India's Rule 10. However, COPPA's threshold of 13 years is substantially lower than the DPDPA's 18-year standard, and critics have long argued that COPPA's protections are easily circumvented through age falsification, a problem equally present in the Indian context.

A critical distinction: COPPA creates a private right of action through FTC enforcement, while the DPDPA channels all complaints through the DPB, which as a newly constituted body faces questions about institutional capacity, staffing, and the speed of adjudication.

C. Synthesis

India's Section 9 aligns broadly with international best practices on the core prohibitions — particularly on behavioural profiling and targeted advertising — areas where the GDPR's own protections have been criticized as insufficiently absolute. Where the DPDPA falls short is in the specificity of age verification infrastructure and the practical operationalization of verifiable consent. The Rules, while an improvement over the draft, still leave the precise mechanics of age verification — including whether Aadhaar-based verification, Virtual IDs, or third-party tokens will suffice — to future executive action and DPB guidance.

V. GAPS, CHALLENGES, AND DOCTRINAL TENSIONS

A. The Age Verification Problem

The most fundamental challenge facing Section 9 is practical: how does a data fiduciary

determine that a user is a child? The DPDP Rules require data fiduciaries to verify whether a person seeking access is a child, but provide limited operational guidance. Children may easily misrepresent their age; parents may assist children in bypassing verification for convenience.

Age verification tools — including document-based verification, biometric checks, or government ID linkage — raise serious counter-concerns around privacy. Requiring every platform user to submit identity documents for age-gating would create vast repositories of sensitive personal data, directly at odds with the data minimization principle that undergirds the DPDPA. This tension between child protection and informational privacy is inherent in any consent-based regime and demands a carefully calibrated regulatory response.

The virtual token mechanism contemplated in the Rules — where tokens mapped to personal data may be used for verification — is promising but presupposes digital literacy and infrastructure that is unevenly distributed across India's population, particularly in rural and semi-urban areas.

B. The Guardianship Verification Problem

Even where a child is correctly identified, verifying that the consenting adult is actually the child's parent or lawful guardian presents a distinct challenge. Indian law recognizes multiple guardianship categories under the Hindu Minority and Guardianship Act, 1956, the Guardians and Wards Act, 1890, and personal law statutes. Requiring data fiduciaries to independently verify guardianship relationships for each processing activity would impose enormous compliance costs and risks being unrealistic for mid-size and small fiduciaries.

Further, the requirement to collect parental identity data may itself conflict with the data minimization principle under Section 6(6) of the DPDPA, which requires that only the data 'necessary for the specified purpose' be collected. Collecting extensive parental identity documentation solely to enable a child to access a gaming or education platform appears disproportionate.

C. Tension with Legitimate Use Grounds

Section 9(1)'s mandatory parental consent requirement creates tension with the 'legitimate use' grounds for processing personal data under Section 7 of the DPDPA — grounds that would ordinarily permit processing without consent for legal obligations, disaster

management, medical emergencies, or court orders. The Act does not expressly address whether legitimate use grounds apply to override the parental consent requirement in Section 9(1). The Fourth Schedule's exemptions partially address this — for instance, exempting healthcare providers and government benefit delivery — but ambiguities remain for emergency and quasi-judicial contexts.

D. Enforcement Infrastructure

The DPB was established as an independent adjudicatory body upon the commencement of Rules on November 13, 2025. However, full operational compliance — including the enforcement of consent and privacy notice requirements — is only expected by May 2027. This 18-month gap creates a window during which children's data remains substantially unprotected by effective enforcement, even as the legal obligations nominally exist.

The DPB's constitution — with only four members — raises concerns about its institutional capacity to handle complaints from India's 560 million internet users. By contrast, the EU's data protection authorities have substantially larger mandates, dedicated enforcement divisions, and stronger investigative powers. India's DPB is a dispute resolution body rather than a proactive supervisory authority, which limits its ability to monitor compliance systematically rather than responding to individual complaints.

E. The Evolving Capacities Gap

International child rights law — including the UN Convention on the Rights of the Child, to which India is a party, and General Comment No. 25 of the Committee on the Rights of the Child (2021) — recognizes the doctrine of 'evolving capacities': the principle that children's autonomy should expand progressively as their maturity grows. India's uniform 18-year threshold does not accommodate this principle. A 17-year-old's data choices are treated identically to a 7-year-old's, with parental gatekeeping applying equally to both.

Section 9(5)'s mechanism — allowing the Central Government to notify lower age thresholds for specific fiduciaries found to process data in a verifiably safe manner — partially addresses this by creating a pathway for differentiated treatment. However, this remains a discretionary executive power rather than a rights-based entitlement for maturing adolescents.

A more robust framework would integrate evolving capacities directly into the statute.

VI. CONCLUSION AND RECOMMENDATIONS

Section 9 of the DPDPA, operationalized through the DPDP Rules, 2025, represents a landmark in India's legislative history — the first statutory recognition that children inhabit a distinct and vulnerable position in the digital data ecosystem. Its core architecture is sound: the verifiable parental consent requirement establishes a substantive rather than formal gatekeeping mechanism; the absolute prohibitions on tracking and targeted advertising reflect globally recognized best practices; and the incentive mechanism under Section 9(5) creates a positive compliance dynamic.

Yet the regime as currently enacted faces substantial implementation challenges. The following recommendations are offered to strengthen it.

First, the government should prioritize the development of a federated, privacy-preserving age verification infrastructure — potentially leveraging the DigiLocker ecosystem — that enables platforms to verify user age without requiring mass collection of identity documents. Standards for what constitutes acceptable age verification should be published as DPB guidance at the earliest opportunity.

Second, the DPB should issue clarificatory guidance on the intersection of the legitimate use grounds under Section 7 and the parental consent requirement under Section 9(1), particularly for healthcare, emergency, and quasi-judicial contexts. Legislative amendment may ultimately be required to explicitly carve out such scenarios.

Third, the 18-year bright-line rule should be revisited in favour of an evolving capacities approach for information society services, consistent with India's obligations under the UNCRC and its General Comment No. 25. A tiered model — analogous to the GDPR's 13-to-16 range with Member State flexibility — would better balance child autonomy with protection.

Fourth, the DPB's institutional capacity should be substantially expanded, with dedicated divisions for child data complaints and proactive audit mechanisms modelled on the UK ICO's enforcement of the Children's Code.

Finally, platforms should be required to build privacy-by-design principles into services likely to be accessed by children — including defaults that deactivate data sharing, profiling, and targeted content algorithms for child users — irrespective of individual consent. The UK AADC's fifteen design standards offer a model that India's DPB could adapt to the domestic context through binding guidelines.

Children's digital rights are not aspirational — they are constitutional. Section 9 provides a strong foundation. The task ahead is to build the institutional, technical, and regulatory architecture that can make it real.

REFERENCES

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

2. Digital Personal Data Protection Rules, 2025 (notified November 14, 2025), Ministry of Electronics and Information Technology, Government of India.

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

4. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

5. Information Technology Act, 2000, No. 21 of 2000 (India).

6. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

7. Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012 (India).

8. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council (25 May 2018).

9. Children's Online Privacy Protection Act, 1998 (United States), 15 U.S.C. §§ 6501–6506.

10. United Kingdom, Information Commissioner's Office, Age Appropriate Design Code (Children's Code) (September 2020).

11. United Nations Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment.

12. United Nations Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990), 1577 UNTS 3.

13. Hindu Minority and Guardianship Act, 1956, No. 32 of 1956 (India).

14. Guardians and Wards Act, 1890, No. 8 of 1890 (India).

15. Nandinii Tandon & Mehul Sharma, 'The Curious Case of Common Consent: Rethinking Verifiable Parental Consent Under the DPDPA, 2023' Law School Policy Review (December

4, 2025).

16. Vikram Jeet Singh & Prashant Mara, 'The Emerging Contours of Verifiable Parental Consent Under India's New Data Privacy Law' International Network of Privacy Law Professionals (2024).

17. Child Rights Clinic, O.P. Jindal Global University, 'Implications on the Data of Children after the Enactment of the DPDPA, 2023' (2024).

18. IAPP, 'With Rules Finalized, India's DPDPA Takes Force' (November 14, 2025).

19. International Association of Privacy Professionals Resource Center, DPDPA Analysis Series (2025).