INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Between Protection and Paternalism: Reconceptualising Children's Data Rights under the DPDP Act, 2023

SOMYA SRIVASTAVA* AND DR SAIF ALI KHAN**

ABSTRACT

Section 9 of the Digital Personal Data Protection Act, 2023 establishes a regime for the processing of children's personal data that is, at first glance, among the most protective in the world. Every individual under eighteen is treated as a "child"; verifiable parental consent is mandatory; tracking, behavioural monitoring, and targeted advertising directed at children are categorically prohibited. The Digital Personal Data Protection Rules, 2025—notified on 13 November 2025—operationalise this regime through Rule 10, which channels parental consent verification through DigiLocker and a virtual-token architecture anchored in government-issued identification. This article argues that the Indian regime, beneath its protective surface, is substantially paternalistic. By treating every adolescent as a child until the eve of her eighteenth birthday, by requiring verifiable parental consent uniformly across the entire under-eighteen population, and by routing verification through state-issued identification, the regime forecloses the participatory and autonomy-respecting dimensions of children's rights that the United Nations Convention on the Rights of the Child and General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment have placed at the centre of the international consensus. Drawing on the doctrine of evolving capacities, comparative regimes (COPPA, GDPR Article 8, the UK Age-Appropriate Design Code), and the constitutional framework of Articles 14 and 21 as elaborated in Puttaswamy, this article proposes a reconceptualisation of children's data rights in India: from a paternalistic regime of binary consent to a tiered, evolving-capacities-based architecture that recognises the participation, autonomy, and access rights of adolescents alongside the protection of younger children.

Keywords: *Digital Personal Data Protection Act 2023; Children's Data Rights; Section 9; DPDP Rules 2025; Rule 10; Verifiable Parental Consent; UN Convention on the Rights of the Child; General Comment No. 25; Evolving Capacities; Age-Appropriate Design.*

* Author is an Assistant Professor at Integral University, Lucknow, Uttar Pradesh, India.
** Author is an Assistant Professor at Integral University, Lucknow, Uttar Pradesh, India

 [ISSN 2581-5369]

I. INTRODUCTION: THE TWO FACES OF PROTECTION

There is a familiar instinct in legislative responses to the dangers of the digital environment for children: when the harms appear acute, the response must be uncompromising. Section 9 of the Digital Personal Data Protection Act, 2023 embodies this instinct in its purest form.[1] For a population of nearly four hundred million minors, [2] the architecture of online life has, in formal terms, been transformed. [3]

It is tempting to read this regime as a triumph of children's data protection. The textual signals are unambiguous: the consent threshold is the highest in any major jurisdiction; the prohibition on tracking and targeted advertising in Section 9(3) is categorical; the verification architecture under Rule 10 is technologically robust. The international literature on children's digital rights has, for two decades, urged precisely this kind of intervention. Why, then, write a chapter that questions the regime?

The argument of this article is that the Indian regime, beneath its protective surface, is paternalistic in ways that undermine the very rights it claims to protect. The international consensus on children's digital rights, crystallised in the United Nations Committee on the Rights of the Child's *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*[4] is not that children must be removed from the digital environment until majority. It is that the digital environment must be re-engineered to accommodate children's evolving capacities, participation rights, and autonomy interests alongside their protection rights. The Indian regime takes the protection branch of this consensus and discards the rest. The result is a framework that, in its zeal to safeguard, may itself constitute a violation of the constitutional and international rights of Indian children.

Three features of the Indian regime warrant particular scrutiny. First, the eighteen-year threshold treats a six-year-old and a seventeen-year-old as legally identical for purposes of digital consent, a treatment that no comparable regime adopts. The United States Children's Online Privacy Protection Act applies only to children under thirteen.[5]The Indian regime stands

[1]Digital Personal Data Protection Act, No. 22 of 2023, s 9, India Code (2023) [hereinafter DPDP Act] (creating special obligations for the processing of personal data of children).
[2]DPDP Act, *supra* note 1, § 2(f) (defining "child" as "an individual who has not completed the age of eighteen years").
[3]Digital Personal Data Protection Rules, 2025, G.S.R. 685(E) (Nov. 13, 2025) [hereinafter DPDP Rules, 2025], r. 10.
[4]U.N. Comm. on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021) [hereinafter *General Comment No. 25*].
[5]Children's Online Privacy Protection Act, 15 U.S.C. ss 6501–6506 (2023) [hereinafter COPPA] (defining "child" as "an individual under the age of 13").

 [ISSN 2581-5369]

alone in its uniform treatment of the entire under-eighteen population. [6]

Second, Rule 10's verification architecture, by routing parental consent through DigiLocker and government-issued virtual tokens, creates a de facto state-identifier requirement for children's online access. [7] The architecture replicates, in the data-protection setting, many of the access and exclusion concerns that animated the Supreme Court's constitutional critique of the Aadhaar regime in *Puttaswamy v. Union of India (Aadhaar-5J.)*. The constitutional question is not whether DigiLocker is a sound verification technology; it is whether channelling all children's digital access through state-issued credentials is a proportionate response to the protection objective.

Third, the Indian regime, by collapsing the entire under-eighteen population into a single category subject to uniform parental consent, forecloses the participation rights that *General Comment No. 25* identifies as a constitutive element of children's digital rights. An adolescent seeking confidential mental-health support, a sixteen-year-old creating a portfolio of original creative work, a seventeen-year-old engaging in civic discourse on online platforms—each of these activities, on the face of the DPDP Act, requires the verifiable consent of the adolescent's parent. The regime treats adolescents as objects of protection rather than as subjects of evolving rights.

This article proposes, in response, a reconceptualisation of children's data rights in India: a tiered, evolving-capacities-based architecture that distinguishes among age bands, calibrates protection to actual harms, and preserves space for adolescent autonomy and participation. The article proceeds in seven Parts. Part II reconstructs the international framework of children's digital rights, with particular attention to the doctrine of evolving capacities. Part III maps the architecture of Section 9 of the DPDP Act and Rule 10 of the 2025 Rules. Part IV develops the comparative critique. Part V interrogates the verification architecture under Rule 10. Part VI evaluates the regime against the constitutional standards of Articles 14 and 21 as elaborated in *Puttaswamy*. Part VII proposes the reform pathway and concludes.

II. THE INTERNATIONAL FRAMEWORK: FROM PROTECTION TO PARTICIPATION

The contemporary law of children's rights, as it bears on the digital environment, rests on a substantive normative architecture that has been developed across more than three decades of

[6]Council Regulation 2016/679, art. 8, 2016 O.J. (L 119) 38 (EU) [hereinafter GDPR] (setting age of digital consent at 16, with Member-State discretion to lower to 13).
[7]Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* (2020) [hereinafter UK AADC].

 [ISSN 2581-5369]

treaty practice, soft-law guidance, and academic theorisation. [8] India, having ratified the United Nations Convention on the Rights of the Child in 1992, is bound by the substantive obligations the Convention imposes. The Indian Majority Act, 1875, like the Convention, fixes the age of majority at eighteen.[9]

The doctrine of evolving capacities, articulated in Article 5 of the Convention, [10]is the doctrinal pivot.[11]

Article 12 of the Convention complements this architecture by guaranteeing the child's right to express views in matters affecting him or her, with due weight given in accordance with age and maturity.[12] Read together, Articles 5, 12, and 16 establish that children's privacy rights are not the property of the parent but of the child, with the parent acting as a facilitator whose role diminishes as the child's capacities evolve.[13]

The most authoritative contemporary articulation of these principles, as applied to the digital environment, is the Committee on the Rights of the Child's *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*[14]

It is important to register what the General Comment does and does not say. It does not say that the protection of children from digital harms is unimportant; on the contrary, it identifies the State's obligation to safeguard children from sexual exploitation, behavioural targeting, and online violence as among the most urgent priorities of contemporary internet governance. What the General Comment says, in the language of paragraph 9, is that "children's rights to non-discrimination, the best interests of the child, life, survival and development, and respect for the views of the child must be central to any legislation, policy or other action concerning the digital environment." Protection is one of these rights; it is not the only one. A regime that treats it as the only one fails the test of children's rights, even where its protective architecture is otherwise well-designed.

This is the doctrinal architecture against which the Indian regime must be measured. It is not the architecture of consumer protection, in which the regulatory question is how high the wall should be built between the protected class and the harms; it is the architecture of children's rights, in which the regulatory question is how the wall can be designed to permit the child's

[8]Indian Majority Act, 1875, No. 9 of 1875, § 3, India Code (1875).
[9]CRC, *supra* note 4, art. 1.
[10]CRC, *supra* note 4, art. 5.
[11]Gerison Lansdown, *The Evolving Capacities of the Child* 5–8 (UNICEF Innocenti Research Centre, 2005).
[12]Id. art. 12.
[13]Id. art. 16.
[14] *General Comment No. 25*, *supra* note 5, ¶ 19.

 [ISSN 2581-5369]

gradual acquisition of agency. The two architectures point, in the Indian setting, in different directions.

The protection–participation tension is not a theoretical abstraction; it has been the central methodological question of children's digital-rights scholarship for over two decades. Sonia Livingstone's influential ethnographic and survey-based work, which formed part of the empirical foundations for the General Comment's drafting, demonstrates that adolescents' digital experiences are constitutively participative: their formation of identity, their development of social and political agency, their pursuit of educational and creative interests, and their negotiation of intimate relationships are each mediated by the digital environment in ways that make uniform parental gatekeeping not merely paternalistic but developmentally counterproductive.[15]

A response common in Indian regulatory discussions is that this international framework, while normatively attractive, is unrealistic for India given the limited digital literacy of Indian parents and the asymmetric power of large technology platforms vis-à-vis Indian children.[16] The argument has surface appeal but does not, on closer examination, support the architecture the DPDP Act has chosen. The argument supports robust protective design (which the General Comment endorses), age-appropriate default settings (which the UK AADC operationalises), and effective enforcement (which the COPPA experience demonstrates is achievable). It does not support the wholesale collapse of differentiated treatment into a single uniform parental-consent regime. The conflation of "robust protection" with "uniform parental consent" is a category error: a robustly protective regime can be differentiated, and a differentiated regime can be robustly protective. The DPDP Act's architectural choice does not fall along that axis.

III. THE ARCHITECTURE OF THE INDIAN REGIME

The Indian regime for children's data has a complex pre-history that informs the present architecture. The Justice B.N. Srikrishna Committee, in its 2018 report, recommended a tiered architecture for children's data, drawing on the international literature on evolving capacities.[17]

The DPDP Act, 2023 collapses the differentiated architecture of the 2019 Bill into a more uniform design. Section 9(1) requires that, before processing any personal data of a child, the data fiduciary "shall … obtain verifiable consent of the parent of such child or the lawful

[15] *See generally* Sonia Livingstone, *Children's Privacy Online*, in *Computers, Phones, and the Internet* 128 (Robert Kraut et al. eds., 2006).
[16] Genevieve Grabman & Yvette Efevbera, *The Tension Between Protection and Participation in Children's Digital Rights*, 30 *Int'l J. Child. Rts.* 421, 428 (2022).
[17] *See* Justice B.N. Srikrishna et al., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 75 (2018) [hereinafter Srikrishna Report].

 [ISSN 2581-5369]

guardian, as the case may be."[18]

Three architectural features deserve close attention. First, the definition of "child" in section 2(f) of the Act—"an individual who has not completed the age of eighteen years"—is uniform across the entire chapter. The Act contains no internal differentiation between younger children and adolescents. Second, the verifiable parental consent requirement applies, on the face of section 9(1), to the processing of any personal data of a child—not merely to commercially or developmentally consequential categories of processing. A seventeen-year-old creating an account on an academic citation manager, signing up for an online university course, or registering for a competitive examination preparation platform is, on the textual reading, subject to the same verifiable parental consent requirement as a six-year-old downloading a game. Third, the section 9(3) prohibition on tracking, behavioural monitoring, and targeted advertising is categorical—not subject to consent-based override—but the Central Government's power under section 9(4) to exempt classes of fiduciaries from these obligations creates an open-ended carve-out whose scope will be determined by future executive notification.

Rule 10 of the DPDP Rules, 2025 operationalises section 9(1)'s verifiable parental consent requirement. Rule 10(1) provides that the consent of the parent must be obtained "by such means … as may enable the Data Fiduciary to verifiably ascertain that … the parent is identifiable."[19]

The aggregate effect of section 9 and Rule 10 is therefore as follows. A data fiduciary that wishes to process the personal data of any individual under eighteen must (i) obtain the verifiable consent of a parent or lawful guardian, (ii) verify the consent through DigiLocker or an analogous government-recognised virtual-token mechanism, and (iii) abstain from any tracking, behavioural monitoring, or targeted advertising directed at the child. The architecture is, formally, exhaustive. Whether it is constitutionally and policy-wise sound is a different question.

It is worth registering, at this stage, the empirical scale of what is at stake. India has, on conservative estimates, more than 250 million minors who are active digital users—across educational technology platforms, gaming services, social media, streaming services, and online learning environments. The pandemic-era expansion of EdTech, which brought platforms such as Byju's, Vedantu, Whitehat Jr., Unacademy, and the government's DIKSHA platform into the homes of every Indian school student, generated vast pools of children's educational and behavioural data that the prior regulatory architecture (the SPDI Rules, 2011) was wholly

[18]DPDP Act, *supra* note 1, § 9(1).
[19]DPDP Rules, 2025, *supra* note 3, r. 10(1).

 [ISSN 2581-5369]

inadequate to govern. The DPDP Act's children's regime is, at one level, a long-overdue response to this empirical reality.

The architectural choice the Act makes, however, may be inadequate to the empirical reality it confronts. Consider three concrete sectoral implications. First, in the EdTech sector, the requirement of verifiable parental consent under Rule 10 creates a barrier to enrolment that disproportionately affects children of digitally-excluded parents. Where the comparator regimes accommodate institutional consent (the school) for educational processing of children's data, the DPDP Act provides no such carve-out. Second, in the mental-health technology sector, the requirement of parental notification of all processing operations forecloses confidential adolescent access to mental-health counselling—a known and documented public-health concern in the Indian setting. Third, in the social-media sector, the categorical prohibition on tracking and behavioural advertising, while substantively warranted, is undermined by section 9(4)'s open-ended carve-out power, which makes the protective architecture vulnerable to executive dilution. The architectural choice is, in each case, both over-protective and under-protective: it imposes excessive parental gatekeeping on benign processing while leaving harmful processing potentially exposed to executive carve-out.

IV. THE COMPARATIVE FRAME: INDIA AS AN OUTLIER

The Indian regime's uniform treatment of the entire under-eighteen population is, when set against the major comparator regimes, an outlier. The comparative analysis is not academic; it bears directly on the constitutional question whether the Indian regime is the "least restrictive alternative" capable of achieving the protection objective.

The United States Children's Online Privacy Protection Act, the longest-standing major children's data protection regime, applies only to children under the age of thirteen.[20]

The General Data Protection Regulation, in Article 8, sets the default age of digital consent at sixteen, with Member-State discretion to lower the threshold to thirteen.[21]

The United Kingdom's Age-Appropriate Design Code, issued by the Information Commissioner's Office in 2020, takes a different approach.

The international comparison reveals three architectural choices that the Indian regime has, in each instance, declined to make. First, no comparator regime treats the entire under-eighteen population as a single category for purposes of digital consent. The age threshold is either lower

[20]COPPA, *supra* note 6, § 6501(1).
[21]GDPR, *supra* note 7, art. 8(1).

 [ISSN 2581-5369]

(COPPA, GDPR with Member-State derogation) or differentiated by age band (UK AADC). Second, no comparator regime channels parental consent verification exclusively through state-issued identification. The COPPA regulations explicitly contemplate multiple verification methods including commercial mechanisms; the GDPR's "reasonable efforts" standard is technology-neutral; the UK AADC requires "robust" age verification but does not specify the mechanism. Third, no comparator regime has a categorical prohibition on tracking, behavioural monitoring, and targeted advertising directed at children. The GDPR's general prohibition on automated decision-making with significant effects (Article 22)[22] applies to children but is subject to specified exceptions; the COPPA framework permits behavioural advertising directed at children only with verifiable parental consent and within prescribed safeguards.

It is worth being clear about what the comparative argument does and does not establish. It does not establish that the Indian regime is normatively wrong; comparative outlier status is not the same as constitutional infirmity. What the comparative argument does establish is that the question whether eighteen is the appropriate threshold, whether state-issued identification is the appropriate verification mechanism, and whether categorical prohibitions are the appropriate regulatory tool has been deliberatively answered in the negative across the major regimes whose architecture India has, in many other respects, sought to emulate. The Indian outlier status thus shifts the analytical burden onto the architects of the Indian regime to justify the divergence. That justification has not, to date, been produced.

V. THE VERIFICATION ARCHITECTURE: RULE 10 AND THE AADHAAR ANXIETY

The verification architecture under Rule 10 of the DPDP Rules, 2025 deserves separate treatment, both because it is the operational core of the Indian children's data regime and because it raises constitutional concerns that the section 9 architecture does not, on its face, raise.

Rule 10(2) specifies, as noted above, that parental verification may proceed through "voluntarily provided details of identity, age and address" verifiable through "a virtual token mapped to such details" issued by an entity entrusted by law or by the Central Government. DigiLocker, in turn, derives its operational legitimacy from the Aadhaar architecture: most DigiLocker authentication flows rely on Aadhaar-based eKYC.

This produces a striking architectural inversion. The Supreme Court in *Justice K.S. Puttaswamy v. Union of India (Aadhaar-5J.)*[23] The Court's reasoning was that the constitutional rights at

[22] *See* GDPR, *supra* note 7, art. 22.
[23] *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.)*, (2019) 1 S.C.C. 1, ¶¶ 244–248 (India).

 [ISSN 2581-5369]

stake—particularly the right to education and the right to access basic services—could not be conditioned on the production of a state-issued biometric identifier where less restrictive alternatives existed. Rule 10, by routing children's digital access through DigiLocker (which is in operational terms an Aadhaar-anchored architecture), reintroduces in the data-protection setting precisely the conditioning that *Puttaswamy II* struck down in the welfare setting.

The exclusion concerns are empirically grounded. The Internet Freedom Foundation has documented that approximately 130 million Indian adults remain without smartphones, and that DigiLocker access is unevenly distributed across urban and rural India.[24] The de facto effect of Rule 10's architecture is therefore that children of digitally-excluded parents face higher barriers to lawful online access than children of digitally-included parents. The barrier is not merely inconvenient; it is constitutionally significant. [25]

A response might be that Rule 10's architecture is technology-neutral on its face, and that data fiduciaries are free to deploy alternative verification mechanisms. The textual reading is plausible, but the operational reality is otherwise. Compliance economics, in the Indian regulatory environment, push fiduciaries toward the verification mechanism that minimises legal risk. DigiLocker, as the government-backed and statute-aligned mechanism, is the default. The Centre for Internet & Society and other stakeholder submissions on the draft 2025 Rules expressly flagged this concern; the final Rules retained the architecture without modification.[26]

A second, related concern is that the verification architecture treats parental consent as a transactional event rather than as an ongoing dimension of the parent-child relationship. Rule 10 provides for verification at the moment of consent collection; it does not, on its face, require any subsequent communication with the parent in respect of changes in processing, addition of new categories of data, or onward transfer to third parties. The architectural assumption is that parental consent, once obtained, is a fixed asset on which the data fiduciary may continue to draw. The contrast with the UK Age-Appropriate Design Code, which embeds the parental relationship into ongoing service design through data minimisation, default high-privacy settings, and parental dashboards, is sharp. The Indian regime's consent architecture is event-based; the international best-practice is relationship-based.

VI. THE CONSTITUTIONAL CASE: ARTICLES 14 AND 21

The constitutional analysis of the Indian regime can be developed under three doctrinal frames:

[24]IFF Submission, 2025, *supra* note 30, at 9–10.
[25]Anumeha Yadav, *The Aadhaar Exclusion Crisis*, Caravan Mag., Sept. 2018.
[26]Centre for Internet & Society, *Comments on the Draft Digital Personal Data Protection Rules, 2025* 14 (Feb. 2025) [hereinafter CIS Comments, 2025].

 [ISSN 2581-5369]

equality before the law under Article 14, the right to privacy and dignity under Article 21 as elaborated in *Puttaswamy*, and—standing in the background—the international-law reception under Article 51(c) of the Constitution

A. Article 14: The Failure of Differentiation

Article 14 of the Constitution guarantees equality before the law and the equal protection of the laws.[27] The Supreme Court has repeatedly affirmed that equal treatment of unequals is itself a violation of Article 14: where persons are differently situated, the law must accommodate the difference, and a uniform rule applied to differently-situated persons is itself a form of discrimination. This doctrinal framework, applied to children's data rights, generates a constitutional difficulty for the DPDP Act's architecture.

The differential cognitive, emotional, and developmental capacities of children at different ages are matters of empirical and developmental-psychological consensus. A six-year-old and a seventeen-year-old are differently situated in respect of every dimension of digital engagement: their capacity to comprehend privacy notices, their capacity to navigate online risks, their capacity to make informed choices about consent, and their stake in the participatory and educational opportunities of the digital environment. The DPDP Act's uniform treatment of the entire under-eighteen population fails to acknowledge these differences. It applies an identical regulatory architecture, verifiable parental consent, categorical prohibition on tracking, blanket exclusion from the participatory dimensions of digital life, to two profoundly differently-situated classes of persons.

The Article 14 challenge is reinforced by the proportionality dimension. The Supreme Court in *Anuradha Bhasin v. Union of India*[28] The protection objective of section 9 is real; the difficulty is that the chosen means, uniform parental consent for all under-eighteens, channelled through state-issued identification, is not the least restrictive alternative. The COPPA threshold of thirteen, the GDPR's sixteen-with-derogation, and the UK AADC's age-banded approach each illustrate that the protection objective can be achieved through architectures that impose lesser restrictions on adolescent autonomy and access. The Indian regime's failure to adopt any of these less-restrictive alternatives is, on the proportionality test, constitutionally suspect.

B. Article 21: Privacy, Dignity, and the Adolescent Subject

Article 21 of the Constitution, as elaborated in the nine-judge bench's decision in *Puttaswamy*

[27]Constitution of India, art. 14.
[28]*Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637, ¶ 64 (India).

 [ISSN 2581-5369]

v. Union of India[29] The Court in *Puttaswamy* was explicit that these rights belong to all persons, including children. Justice Chandrachud's lead judgment grounded the privacy right in dignity; dignity, in turn, was understood to attach to the person as a developing subject capable of self-authorship.

The Article 21 difficulty with the DPDP Act's children's regime is that it constitutes adolescents as objects of parental decision-making rather than as developing subjects of self-determination. An adolescent's right to access mental-health support online without parental notification, to engage in confidential reproductive-health consultation, to seek information on sexual orientation and gender identity, to engage in civic discourse, or to develop a creative or professional online presence are each implicated by the section 9(1) architecture. The Mental Healthcare Act, 2017 explicitly recognises the right to confidentiality applicable to all persons, including minors;[30] The DPDP Act's parental-consent regime cuts across these sectoral protections. [31]

The Supreme Court's decision in *X v. Principal Secretary, Health and Family Welfare Department, Govt. of NCT of Delhi*[32] The Court held that the constitutional right to bodily autonomy is not contingent on adult majority; it attaches to the person in proportion to her capacity to exercise it. The architectural commitment underlying this judgment—that constitutional rights must be calibrated to evolving capacities, not to chronological thresholds—is the very commitment that the DPDP Act's children's regime fails to make.

The Kerala High Court's decision in *Faheema Shirin v. State of Kerala*[33] The Court there recognised the right to access the internet as a facet of the right to education and the right to privacy under Article 21. The recognition is significant for the present analysis: where the right to access digital information is itself a constitutional right, the State's power to condition that access on the production of state-issued credentials cannot be unconditional. It must satisfy the proportionality standard. Rule 10's effective conditioning of children's digital access on DigiLocker-mediated parental verification, where the available alternatives—commercial verification methods, risk-calibrated self-attestation, age-banded design—have not been adopted, fails the proportionality test.

[29]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India) [hereinafter *Puttaswamy*].
[30]Mental Healthcare Act, No. 10 of 2017, § 23(1).
[31]Telemedicine Practice Guidelines, Notification No. MCI-211(2)/2019(Ethics)/100659 (Mar. 25, 2020), Indian Medical Council, App. 5, ¶ 3.7.1.
[32]*X v. Principal Secretary, Health and Family Welfare Department, Govt. of NCT of Delhi*, (2023) 9 S.C.C. 433 (India).
[33]*Faheema Shirin v. State of Kerala*, 2019 SCC OnLine Ker 2976, ¶ 14.

A further dimension of the Article 21 analysis concerns the *horizontal* application of the privacy right. The DPDP Act's regime, by requiring parental consent for the processing of all under-eighteen personal data, treats the parent–child privacy relationship as one of unilateral parental decision-making. The constitutional understanding of privacy in India, particularly as developed in *Puttaswamy*, is more nuanced. Privacy is, on the constitutional understanding, an individual right that attaches to each person; the parent–child relationship moderates but does not extinguish the child's privacy claim against intrusion, including parental intrusion. A regulatory architecture that fails to recognise the child's independent privacy interest vis-à-vis the parent—particularly in domains such as mental health, sexuality, gender identity, and political expression—imports a vision of the parent–child relationship that the Constitution does not endorse.

C. Article 51(c): The International-Law Reception

Article 51(c) of the Constitution directs the State to "foster respect for international law and treaty obligations." The provision is, formally, a non-justiciable directive principle, but the Supreme Court has repeatedly drawn on it to inform constitutional interpretation, particularly where international human-rights obligations are at issue. India's ratification of the Convention on the Rights of the Child generates an obligation to give effect to the substantive protections of the Convention, including Article 5's evolving-capacities doctrine, Article 12's participation right, and Article 16's privacy right. The DPDP Act's children's regime, by collapsing the differentiated architecture that the Convention requires into a uniform parental-consent regime, fails to give effect to these obligations. Whether this failure is, in itself, a justiciable constitutional violation is a question the courts will need to address; what is clear is that the Article 51(c) reception of the Convention generates an interpretive presumption against the uniform regime and in favour of the differentiated architecture that the Convention contemplates.

VII. The path forward: a tiered architecture for Indian children's digital rights

The reform pathway sketched here operates on the premise that the protection objective of section 9 is legitimate and important, and that the architectural difficulty is not the existence of children's data protection but its design. The proposed reforms are, in this sense, reformist rather than abolitionist: they preserve the substantive commitments of the DPDP Act while reconfiguring the architecture to accommodate evolving capacities, participation, and access.

The first reform pathway, and the most modest, is administrative differentiation under section

9(5). The provision authorises the Central Government to notify, in respect of any data fiduciary that has ensured "verifiably safe" processing, the age above which the verifiable parental consent requirement does not apply.[34] The provision was, in legislative debates, conceived as a fallback for sectoral exemptions. It can, on the analysis offered here, do considerably more work. A general notification fixing the threshold at sixteen for educational, mental-health, civic-engagement, and creative-platform fiduciaries would substantially reduce the over-inclusiveness of the regime without legislative amendment. The administrative pathway is doctrinally clean and politically tractable.

The second reform pathway is rule-based age banding. The DPDP Rules, 2025 already contain the operational machinery for differentiated treatment; what they lack is the substantive architecture. A rule revision modelled on the UK Age-Appropriate Design Code—prescribing differentiated obligations for fiduciaries serving children aged 0–5, 6–12, 13–15, and 16–17—would preserve the protective architecture for younger children while opening up appropriate participatory space for adolescents. The verification mechanism under Rule 10 could similarly be calibrated: stricter verification (state-issued identification) for younger children, less restrictive mechanisms (commercial methods, self-attestation with risk-based audit) for older adolescents.

The third reform pathway, more ambitious, is statutory amendment. Parliament could amend the DPDP Act to redefine "child" for purposes of the Act as a person below sixteen years of age, with a graduated consent regime for adolescents aged sixteen and seventeen. Such an amendment would align the Indian regime with the GDPR default, bring it within the centre of gravity of the international consensus, and resolve the constitutional difficulties identified in Part VI without dismantling the protective architecture for younger children. The amendment would require complementary changes to ensure that the section 9(3) prohibition on tracking and behavioural advertising continues to apply to all under-eighteens, since the harms of behavioural advertising are not eliminated at age sixteen.

A fourth pathway, and one that should accompany whichever of the first three is chosen, is the development of an age-appropriate-design code for India. The UK's Information Commissioner's Office's code is the leading global model;[35] an Indian equivalent, issued by the Data Protection Board under section 27 of the DPDP Act or by the Ministry of Electronics and Information Technology, would provide the operational guidance that the textual provisions of

[34]DPDP Act, *supra* note 1, § 9(5).

 [ISSN 2581-5369]

the Act cannot. Such a code would address the operational realities of contemporary children's digital life-gaming, EdTech, social media, online learning, in ways that the text of the Act, by its nature, cannot.

A fifth, complementary pathway lies through litigation. A constitutionally framed petition under Article 32, challenging the uniform application of section 9(1) to the entire under-eighteen population on Articles 14 and 21 grounds, can proceed on the analysis offered here. The relief sought would not be the striking-down of the children's regime but a declaration that the regime, as currently designed, is constitutionally over-inclusive, coupled with a direction to the Union of India to differentiate the architecture by age band. The technique is analogous to the social-action litigation in *Vishaka v. State of Rajasthan*, where the Court issued interim guidelines pending legislative action. The constitutional Court has, in recent years, shown increasing willingness to engage with such structural challenges; the children's data regime presents a particularly compelling occasion.

VIII. Conclusion

The Digital Personal Data Protection Act, 2023 is, in its commitment to protecting children from digital harms, an overdue and important statute. Its categorical prohibition on tracking, behavioural monitoring, and targeted advertising directed at children, in particular, represents a substantive advance on the architecture of regulatory non-protection that preceded it. Few would deny that the harms the Act seeks to address—commercial surveillance of children, behavioural manipulation, addictive design, and the erosion of childhood as a developmentally protected space—are real, urgent, and constitutionally significant.

The architectural choice, however, has been made in a register that this article has called paternalistic. By collapsing the entire under-eighteen population into a single category, by requiring uniform verifiable parental consent across the population, and by channelling verification through a state-anchored identification architecture, the regime privileges the protective dimension of children's rights at the expense of the participatory and access dimensions. The international consensus, as articulated in *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, does not endorse this trade-off. The comparative regimes—COPPA in the United States, GDPR Article 8 in the European Union, the UK Age-Appropriate Design Code—each reject it. The Indian constitutional framework, as elaborated in *Puttaswamy* and *Anuradha Bhasin*, supplies the doctrinal materials for rejecting it as well.

The reconceptualisation proposed here is modest in its ambition but consequential in its

 [ISSN 2581-5369]

architecture: a tiered, evolving-capacities-based regime that calibrates protection to age band, preserves space for adolescent autonomy and participation, and retains the categorical prohibitions on the most harmful forms of children's data processing. The reform pathway can be travelled in stages—administrative notification under section 9(5), rule-based age banding, statutory amendment, age-appropriate design code, and constitutional litigation. None of these pathways is exclusive; together, they offer a route by which the Indian regime can move from a paternalistic regime of binary consent to a children's rights regime worthy of the international consensus to which India has, by its ratification of the Convention on the Rights of the Child, already committed.

The constitutional question raised by the present regime is not whether children's data deserves protection. It does. The question is whether the architecture chosen is the architecture that the constitutional and international framework permits. On the analysis offered here, the answer is no. The reform pathway is available; the constitutional and policy case for taking it is, at the moment of the DPDP Rules' commencement, more pressing than it has ever been. The choice between protection and participation is, ultimately, a false one. The constitutional task is to design a regime that delivers both.

*****

 [ISSN 2581-5369]