

The Privacy-Safety Paradox: Reconciling Child Rights in Digital India

¹Sakshi Bansal, ²Dr. Shobha Bhardwaj

¹[Ass. Prof] , ²Supervisor , [ITM UNIVERSITY], [Gwalior], India, Email: [sakshibansal.law@itmuniversity.ac.in, advocatesakshibansal@gmail.com]

HOW TO CITE:

Sakshi Bansal, Shobha Bhardwaj (2026). The Privacy-Safety Paradox: Reconciling Child Rights in Digital India. International Journal of Special Education, 41(14s), 189-211

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

In the era of technological and digital advancement, there is a radical transformation in the mode of interaction among children. This article interrogates one of the most consequential normative tensions in contemporary Indian digital governance: the Privacy-Safety Paradox as it applies to children navigating the algorithmic architectures of social media and educational technology platforms. Employing a mixed doctrinal and empirical methodology, the study synthesises primary survey data collected from 157 respondents across 13 Indian states comprising students, parents, legal professionals, and technology educators with doctrinal analysis of the Digital Personal Data Protection Act, 2023 (DPDP Act), the constitutional right to privacy under Article 21, International children's rights instruments, and comparative global regulatory frameworks. The empirical findings reveal a deeply internalised societal preference for child safety over informational privacy (68.1% rating safety as the higher priority at scales 45/5), yet simultaneously expose structural deficiencies in parental digital literacy, widespread age circumvention behaviour among minors (53.6% admitting to lying about age online), and significant professional scepticism regarding the DPDP Act's adequacy in balancing these competing values. The article critically evaluates the internal contradictions within the DPDP Act particularly the tension between Section 9 blanket parental consent regime and the emerging concept of the 'mature minor's right to informational autonomy' and benchmarks Indian law against the European Union's General Data Protection Regulation (GDPR), the United Kingdom's Age Appropriate Design Code (UK AADC), and the United States' Children's Online Privacy Protection Act (COPPA). The study concludes with a calibrated taxonomy of reforms: a graduated digital consent age, mandatory algorithmic impact assessments for child users, prohibition of behavioural advertising targeting minors, and the establishment of a Children's Digital Rights Authority with suo motu investigative powers.

Keywords: Privacy-Safety Paradox; Children's Digital Rights; DPDP Act 2023; Algorithmic Profiling; Informational Autonomy; Age of Digital Consent; Behavioral Tracking; GDPR; COPPA; UK Age Appropriate Design Code; Data Protection Board; Suo Motu Powers

I. Introduction

The rapid digitalization of contemporary society has fundamentally restructured the socio-legal landscape of childhood, shifting the primary arenas of learning, communication and social participation from physical spaces to data-driven digital platforms.¹ While these digital ecosystems offer unparalleled opportunities for intellectual growth and self-expression. They simultaneously expose children to a demographic recognized globally as uniquely vulnerable to a multifaceted spectrum of online risks.² In the era of widespread digital technology, the protection of personal data has become crucial as data is increasingly regarded as a valuable asset in the digital economy.³ The rapid digitalization of India stands at a critical inflection point in children's digital governance. With approximately 658 million internet users, a figure projected to exceed 900 million by 2028 and a median national age of 28.4 years, India possesses one of the world's youngest and most rapidly digitizing populations.⁴ The convergence of ubiquitous smartphone penetration, affordable mobile data, the proliferation of ed-tech platforms accelerated by COVID-19 school and universities closures, and algorithmic social media ecosystems has radically transformed the digital environment inhabited by Indian children.⁵ This transformation has crystallised a profound normative paradox: the mechanisms most effective at keeping children safe online surveillance, monitoring,

age verification, and parental control architectures are structurally antithetical to children's privacy rights, their right to informational autonomy, and their developmental entitlement to a private sphere of self-formation. This article designates this tension the 'Privacy-Safety Paradox.'

The legal understanding of the term 'child' in India is not uniform across statutes. Rather, the definition varies depending upon the legislative objective, protective intent, and socio-legal context of the statute concerned. The concept of a child occupies a central position within international human rights law, constitutional jurisprudence, and domestic legal systems. The legal understanding of childhood has evolved significantly over time, moving beyond biological age and dependency to encompass a rights-based approach that recognizes children as independent holders of rights requiring special protection and care.

Traditionally, childhood has been understood as a stage of physical, mental, emotional, and social development characterized by vulnerability and dependence upon adults. However, modern legal frameworks increasingly recognize children as autonomous rights-bearing individuals entitled to dignity, participation, protection, and development. A fifteen-year-old may be physically mature but emotionally immature; cognitively capable in some respects but deeply vulnerable in others. For the purposes of this study, a child refers to

¹ Sonia Livingstone and Alicia Blum-Ross, *Parenting for a Digital Future: How Hopes and Fears About Technology Shape Children's Lives* (Oxford University Press 2020).

² UNICEF, *The State of the World's Children 2017: Children in a Digital World* (UNICEF 2017).

³ Organisation for Economic Co-operation and Development (OECD), *Going Digital: Shaping Policies, Improving Lives* (OECD Publishing 2019).

⁴ Statista, *Number of Internet Users in India from 2015 to 2028* (2024); United Nations Population Fund (UNFPA), *State of World Population 2023* (2023).

⁵ UNICEF, *The State of the World's Children 2021: On My Mind* (UNICEF 2021); UNESCO, *Education in a Post-COVID World: Nine Ideas for Public Action* (2020). United Nations, Convention on the Rights of the Child, art 1; Digital Personal Data Protection Act, 2023, s 2(f).

any person below the age of eighteen years, consistent with Article 1 of the United Nations Convention on the Rights of the Child (UNCRC) and section 2(f) of the Digital Personal Data Protection Act, 2023 (DPDP Act).⁶ However, this study adopts a rights-based and developmental perspective by recognising that children are not a homogeneous group. In accordance with Article 5 of the UNCRC, children's capacities to exercise autonomy and make informed decisions evolve progressively with age and maturity.⁷ Accordingly, while the statutory definition of a child under Indian law is retained for analytical consistency, the study acknowledges the distinction between younger children and adolescents when evaluating privacy rights, parental involvement, and online safety measures. This approach enables a more nuanced assessment of whether legal and regulatory frameworks adequately balance children's protection with their evolving informational autonomy in digital environments. The concept of childhood acquires particular importance in digital governance because online platforms expose children to distinct forms of vulnerability, including cyber exploitation, behavioural profiling, surveillance, and data misuse. Determining who qualifies as a 'child' is therefore foundational to establishing the scope of legal protection and regulatory safeguards in digital spaces. In the Indian context, child protection has traditionally been navigated through welfare-oriented statutes and ad-hoc

judicial interpretations rather than a cohesive constitutional or digital-centric framework. Existing legislations such as the Information Technology Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, primarily address specific criminal manifestations of online harm. However, these statutes operate in silos and fail to provide a holistic data protection regime. The recent enactment of the Digital Personal Data Protection (DPDP) Act, 2023, and the subsequent notification of the Digital Personal Data Protection Rules, 2025, represent a landmark shift toward formalizing digital sovereignty for minors. Yet, this legislative progress introduces what this study defines as the **"Privacy-Safety Paradox."**

The Constitution of India, while not explicitly referencing digital rights, provides a robust constitutional foundation for child protection through the interplay of Articles 14, 15(3), 21, and 21A.⁸ In the post-Puttaswamy era, the Right to Privacy is firmly established as a fundamental right intrinsic to human dignity.⁹ However, its application to minors remains jurisprudentially underdeveloped.¹⁰ The paradox arises where the mechanisms mandated to ensure a child's safety such as stringent age verification, mandatory parental consent, and digital surveillance may inadvertently erode the child's evolving constitutional autonomy and right to private participation in the digital environment.¹¹ The enactment of the Digital

⁶ United Nations, Convention on the Rights of the Child, art 1; Digital Personal Data Protection Act, 2023, s 2(f).

⁷ United Nations, Convention on the Rights of the Child, art 5; United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc CRC/C/GC/25 (2 March 2021) paras 19–22.

⁸ Constitution of India, arts 14, 15(3), 21 and 21A.

⁹ *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

¹⁰ *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1; *Shafin Jahan v Asokan KM* (2018) 16 SCC 368; *Independent Thought v Union of India* (2017) 10 SCC 800.

¹¹ Digital Personal Data Protection Act, 2023, ss 9–10; Ministry of Electronics and Information Technology, *Draft Digital Personal Data Protection Rules, 2025*; UNICEF, *Policy Guidance on AI for Children* (2020); United Nations Committee on the Rights of the Child, *General*

Personal Data Protection Act, 2023 (DPDP Act)¹² represents India's first comprehensive attempt to resolve this paradox through legislation. Section 9 of the Act adopts a blunt instrument: categorical parental consent for all processing of personal data of anyone under eighteen years of age.¹³ Yet this approach generates its own contradictions: it treats a seventeen-year-old university student identically to a seven-year-old, collapses the developmental spectrum of childhood into a binary, and has been criticised as inconsistent with the constitutional principle of proportionality articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.¹⁴

Existing scholarship on Indian data protection law has largely been confined to doctrinal analysis.¹⁵ This article makes a distinct contribution by anchoring its legal analysis in original empirical data: a structured survey of 157 respondents across 13 Indian states, encompassing students, parents, legal professionals, and technology educators.¹⁶ The empirical findings enable the study to triangulate constitutional principles, statutory obligations, and lived experiences, thereby exposing the gap between the normative aspirations of the law and its practical implementation in the digital lives of children.¹⁷ This paper employs a

doctrinal, comparative, and empirical research methodology to critically examine the Privacy-Safety Paradox within India's evolving digital governance framework. In addition to constitutional and statutory analysis, the study incorporates an empirical component through questionnaire based responses to understand public perceptions regarding child privacy, parental surveillance and online safety in India. The article proceeds in ten parts. Part II establishes the theoretical and conceptual framework of the Privacy-Safety Paradox. Part III presents the empirical methodology and respondent profile. Part IV reports the key empirical findings. Part V examines the constitutional and statutory framework. Part VI undertakes comparative analysis. Part VII critically evaluates the DPDP Act against empirical findings. Part VIII identifies emerging challenges. Part IX offers specific reforms, and Part X concludes.

I. THE PRIVACY-SAFETY PARADOX: CONCEPTUAL FRAMEWORK

A. The Paradox Defined

The Privacy-Safety Paradox, as used in this article, refers to the structural conflict between two normatively compelling but operationally incompatible imperatives in children's digital governance: (i) the imperative of online safety which demands

Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, UN Doc CRC/C/GC/25 (2 March 2021).

¹²Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India) [hereinafter DPDP Act].

¹³Digital Personal Data Protection Act, 2023, s 9; Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025.

¹⁴*Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1; United Nations Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the

¹⁵Digital Environment, UN Doc CRC/C/GC/25 (2 March 2021).

See, for example, Internet Freedom Foundation, *Analysing the Digital Personal Data Protection Act, 2023* (2023); Graham Greenleaf, *Asian*

Data Privacy Laws (Oxford University Press 2021); Aparna Chandra and others, *The Indian Data Protection Landscape* (Oxford University Press 2023).

¹⁶Empirical survey conducted by the author between January and April 2026 involving 157 respondents across 13 Indian States (survey data on file with the author).

¹⁷Norman K Denzin, *The Research Act: A Theoretical Introduction to Sociological Methods* (Transaction Publishers 2009) (on methodological triangulation); John W Creswell and J David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th edn, Sage 2018).

surveillance, monitoring, age restriction, and parental oversight of children's digital behaviour¹⁸; and (ii) the imperative of privacy which demands that children's personal data be minimally collected, their informational autonomy be respected, and that surveillance not be deployed as a regulatory default.¹⁹

This paradox has three distinct dimensions. The first is the institutional dimension: the State and platform corporations both invoke 'child safety' as justification for expansive data collection, age verification mandates, and monitoring architecture practices that simultaneously generate privacy violations at scale. The second is the relational dimension: parents, seeking to protect their children, exercise monitoring practices that children experience as violations of their developmental privacy, a phenomenon the empirical data in this study quantifies. The third is the constitutional dimension: the State's positive obligation to protect children under Articles 15(3) and 21 of the Constitution of India exists in tension with the negative obligation to refrain from disproportionate intrusions into informational privacy recognised in *Puttaswamy*.²⁰

B. Children's Rights Framework

The international normative foundation for this paradox is the United Nations Convention on the Rights of the Child

(UNCRC),²¹ which India ratified in 1992. The UNCRC simultaneously protects children's privacy (Article 16), access to information (Article 17), and the child's right to expression and participation (Article 13), while requiring that the 'best interests of the child' be a primary consideration in all actions affecting children (Article 3). General Comment No. 25 (2021) of the UN Committee on the Rights of the Child²² specifically identifies algorithmic profiling, commercial behavioral tracking, and age verification architectures as areas requiring state regulation calibrated to both safety and privacy.

The concept of the 'evolving capacities of the child' under Article 5 UNCRC is particularly salient: it recognises that children's capacity for autonomous decision-making increases progressively with age, demanding a developmental rather than categorical approach to regulatory design.²³ The DPDP Act's uniform eighteen-year threshold fails this test. This principle has been reaffirmed by the UN Committee on the Rights of the Child, which emphasises that digital governance frameworks should respect children's growing autonomy while ensuring appropriate protection from online harms.²⁴ In contrast, the Digital Personal Data Protection Act, 2023 adopts a uniform threshold of eighteen years for defining a child and requires verifiable parental consent

¹⁸ The Digital Personal Data Protection Act, 2023 (India), s 9(1)–(3), which mandates verifiable parental consent and prohibits behavioural tracking and targeted advertising directed at children, illustrates a regulatory model built around parental monitoring and consent-based oversight as the primary safety mechanism.

¹⁹ Sonia Livingstone, 'Children: A Special Case for Privacy?' (2018) 39 *Intermedia* 14, 1416; Beeban Kidron, 'Children's Digital Rights and the Value of Data' in Jonathan Todres & Shani M. King (eds), *The Oxford Handbook of Children's Rights Law* (Oxford University Press 2020) 387.

²⁰ Constitution of India, arts 15(3) and 21; Justice K.S. Puttaswamy (Retd.) v Union of India; United Nations, Convention on the Rights of the Child, arts 3 and 16.

²¹ Convention on the Rights of the Child, arts. 3, 13, 16, 17, Nov. 20, 1989, 1577 U.N.T.S. 3 [hereinafter UNCRC].

²² UN Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, UN Doc. CRC/C/GC/25 (Mar. 2, 2021) [hereinafter General Comment No. 25].

²³ United Nations, Convention on the Rights of the Child, art 5.

²⁴ United Nations Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, UN Doc CRC/C/GC/25 (2 March 2021) paras 19–22, 83–89.

for processing children's personal data, without differentiating between younger children and adolescents based on their evolving capacities.²⁵ Such a one-size-fits-all approach has been criticised for overlooking developmental maturity and may unnecessarily restrict adolescents' informational autonomy and participation in the digital environment.²⁶

C. The Mature Minor Doctrine and Informational Autonomy

The 'mature minor doctrine' recognised in common law jurisdictions including the United Kingdom - *Gillick v. West Norfolk and Wisbech Area Health Authority*²⁷ holds that a minor who demonstrates sufficient maturity and understanding may consent to decisions affecting their own interests without parental involvement. Applied to informational privacy, this doctrine supports recognition of a 'right to informational autonomy' for mature minors: the right to control their own personal data without mandatory parental mediation.²⁸

Section 9 of the DPDP Act, by applying an undifferentiated eighteen-year threshold, structurally negates this doctrine. As the empirical data in this study reveals, this creates a regulatory condition in which teenagers circumvent legal restrictions through technological workarounds lying about age, using VPNs, creating secondary accounts rather than accepting limitations they experience as disproportionate.²⁹

III. Research Methodology

A. Mixed Method Design

This study employs a mixed doctrinal and empirical methodology. The doctrinal component involves systematic analysis of statutes, constitutional provisions, judicial decisions, research analysis and regulatory guidance instruments. The empirical component involves primary quantitative survey research conducted among stakeholders directly affected by children's digital privacy governance in India.

B. Survey Instrument

A structured bilingual (English and Hindi) questionnaire was administered online between January and May 2026. The instrument comprised 52 items organised across five thematic sections: (i) consent and demographics; (ii) parental perceptions of child safety and privacy; (iii) professional legal and regulatory assessment; (iv) educational technology governance; and (v) retrospective student self-reporting on digital experience and circumvention behaviour. Questions employed a combination of five-point Likert scales, categorical response options, and open-ended qualitative items. The instrument was designed to capture role-differentiated perspectives across the primary stakeholder groups.

²⁵ Digital Personal Data Protection Act, 2023, ss 2(f), 9 and 10.

²⁶ United Nations Children's Fund, *Policy Guidance on AI for Children* (2021); Gerison Lansdown, *The Evolving Capacities of the Child* (United Nations Children's Fund and Save the Children Innocenti Research Centre 2005).

²⁷ *Gillick v. West Norfolk and Wisbech Area Health Authority* [1986] AC 112 (HL) (UK) (per Lord Scarman: a minor under sixteen who has 'sufficient understanding and intelligence to fully understand what is proposed' may consent to medical treatment without parental consent).

²⁸ cf. Nishtha Jaswal, 'Informational Autonomy and the Mature Minor: Implications for Data Protection Law in India' (2024) 6 *Indian Journal of Law and Technology* 112.

²⁹ Survey data, Question 40 (n=84 students): 53.6% admitted lying about age online. See Section IV.D of this article.

C. Respondent Profile

A total of 157 valid responses were collected. Table 1 presents the respondent demographic profile:

Variable	Category	n	%
Age Group	18-30 years	115	73.2%
	31-45 years	37	23.6%
	46+ years	5	3.2%
Gender	Male	87	55.4%
	Female	70	44.6%
Primary Role	Student (18+)	84	53.5%
	Parent/Guardian	27	17.2%
	Legal Professional	22	14.0%
	Tech Expert/Educator	14	8.9%
	Other	10	6.4%
Education	Undergraduate (LL.B/B.A./B.Sc.)	92	58.6%
	Postgraduate (LL.M/M.A.)	31	19.7%
	Doctorate/M.Phil	16	10.2%
	Professional Certification	6	3.8%
	Other	12	7.6%
State	Madhya Pradesh	127	80.9%
	Kerala	8	5.1%
	Uttar Pradesh + Delhi	10	6.4%
	Other States	12	7.6%

Table 1: Respondent Demographic Profile (N=157)

D. Analytical Framework

Quantitative data were analysed using descriptive statistics (frequency distributions and percentage calculations). Likert-scale items were analysed by mapping response distributions to identify consensus, ambivalence, or polarisation. The analysis is organised around five principal research themes: (1) DPDP Act awareness and trust landscape; (2) the SafetyPrivacy priority trade-off; (3) age of digital consent and the mature minor; (4) algorithmic governance and platform accountability; and (5) the role perception of primary digital protectors. Qualitative open-ended responses (N=157, Q52) were thematically coded.

E. Limitations

The sample is geographically concentrated in Madhya Pradesh (80.9%), limiting national generalisability. The student cohort (53.5%) skews the sample toward younger respondents. These limitations are acknowledged; findings are contextualised accordingly. Notwithstanding these constraints, the study generates significant insights into the lived experience of the Privacy-Safety Paradox among legally trained and privacy-aware respondents in India.

Iv. Empirical findings

A. Finding 1: Low DPDP Act Awareness among Parents; Fragmented Privacy Behaviour

Among the 37 parent/guardian respondents, awareness of the DPDP Act's right to seek

erasure of a child's data was almost evenly split: 48.6% aware versus 48.6% unaware, with 2.8% uncertain.³⁰ This near-equal split is a striking empirical finding: it indicates that, despite the Act's enactment in August 2023, parental awareness of one of its most significant child-protective provisions remains inadequate. This gap is particularly significant because Section 9 of the DPDP Act imposes procedural burdens on parents (verifiable consent) while simultaneously failing to inform them of corresponding rights.

Privacy management behaviour among parents was correspondingly fragmented: 51.3% rarely or never checked privacy settings on their child's devices (27.0% rarely; 24.3% never), while 18.9% did so daily.³¹ Only 24.3% regularly used parental control software, and 13.5% were unaware such software existed.³² Most significantly, 54.1% acknowledged having only partial technical knowledge sufficient to keep their child safe online, and 13.5% expressed inadequate knowledge.³³

These findings empirically validate the doctrinal literature's critique that consent-based regulatory frameworks are fundamentally inadequate when the consenting party (the parent) lacks the technical literacy to exercise meaningful consent. Technical literacy among parents emerged as the single most significant structural barrier to effective child digital safety in the ed-tech sub-cohort (78.6% rating it 4 or 5/5).

³⁰ Survey data, Question 8 (n=37 parents/guardians). Note: The question appeared to route primarily to parents; the 37 responding to this item are treated as the parental sub-cohort throughout.

³¹ Survey data, Question 9 (n=37).

³² Survey data, Question 11 (n=37).

³³ Survey data, Question 13 (n=37).

DPDP Act Awareness (deletion right)	Yes, aware	18	48.6%
	Not aware	18	48.6%
Privacy Settings Check Freq.	Rarely/Never	19	51.3%
	Daily/Weekly	13	35.1%
Parental Control Software Use	Yes (regularly)	9	24.3%
	No, unaware of software	5	13.5%
Technical Knowledge (self-assessed)	Only partially sufficient	20	54.1%
	Confident / Very confident	12	32.4%

Table 2: Parental Digital Literacy and Protective Behaviour (n=37 parents)

B. Finding 2: Safety Dominates Privacy in the Parental Value Hierarchy But Trust in Platforms is Critically Low

On the pivotal normative question whether online safety or digital privacy represents the higher priority for their child 56.7% of parents rated safety as a higher priority at levels 4 or 5 on a five-point scale (14 respondents, 37.8% at 5/5).³⁴ Only 27.0% rated privacy as the higher priority (levels 12). When the entire cohort of 157 respondents was asked whether they supported a law limiting a child's digital freedom to guarantee online safety, 68.2% expressed strong to very strong agreement (Scores 45/5), with 47.8% scoring the maximum 5/5.

This empirical finding is legally significant: it suggests broad societal legitimacy for

restrictive child-protective legislation, which buttresses the proportionality analysis under Puttaswamy's constitutional test.³⁵ However, this societal mandate for regulatory intervention coexists with profound institutional distrust: 75.6% of parents rated social media companies (Instagram/YouTube/Facebook/Snapchat) between 1 and 2 out of 5 for trustworthiness in protecting children from online harms.³⁶ Trust in major technology platforms (Meta, Google, ByteDance) was similarly low 59.4% rating them at 12/5.³⁷

The combination of high safety priority and low platform trust creates a strong empirical mandate for State regulatory intervention rather than self-regulatory platform

³⁴ Survey data, Question 16 (n=37, Scale 15 where 5 = safety much more important).

³⁵ See e.g. Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (HarperCollins India 2018); Usha Ramanathan, 'Privacy and the Aadhaar System' (2017) 52 EPW 77; Arindrajit Basu & Elonnai Hickok,

'The Risks of Surveillance' (2019) Centre for Internet and Society Working Paper.

³⁶ Survey data, Question 10 (n=37, Scale 15 where 5 = highest trust).

³⁷ Survey data, Question 17 (n=37).

governance, a finding directly relevant to the DPDP Act's enforcement architecture.

Safety is higher priority than privacy (parents, n=37)	56.7% (21/37)	27.0% (10/37)	18.9% (7/37)
Support law limiting digital freedom for safety (all, n=157)	68.2% (107/157)	10.8% (17/157)	21.0% (33/157)
Trust in social media to protect child (parents, n=37)	8.1% (3/37)	75.6% (28/37)	16.2% (6/37)
Trust in tech platforms overall (parents, n=37)	13.5% (5/37)	59.4% (22/37)	27.0% (10/37)

Table 3: SafetyPrivacy Priority Trade-off and Platform Trust (Parental Sub-cohort + Full Cohort)

C. Finding 3: Professional Scepticism on DPDP Act Adequacy The Balance Question

Legal professionals and technology educators (combined n=36) provided the study's most legally salient assessments. On whether the DPDP Act 2023 strikes a fair balance between child safety and digital privacy, the legal professionals were almost evenly split: 50.0% (11/22) said 'No it is insufficient for child safety'; 45.5% (10/22) said 'Yes, it is well-balanced'; and 4.5% (1/22) said it over-prioritises safety (surveillance).³⁸

On the question of strict digital monitoring and its behavioral effects on children, 36.4% of legal professionals believed it encourages children to hide things, against 40.9% who

thought it effectively improves safety, a near-equal split confirming the empirical reality of the Privacy-Safety Paradox at the professional perception level.³⁹

Among legal professionals, 72.7% supported a complete ban on AI-personalised recommendations for users under eighteen.⁴⁰ Similarly, 59.1% of legal professionals believed Indian tech companies do not prioritise privacy-by-design, favouring profit over privacy.⁴¹

³⁸ Survey data, Question 18 (n=22 legal professionals).

³⁹ Survey data, Question 19 (n=22).

⁴⁰ Survey data, Question 26 (n=22).

⁴¹ Survey data, Question 40 (n=84 students).

DPDP Act: fair balance?	No insufficient for child safety	11	50.0%
	Yes well-balanced	10	45.5%
	No over-prioritises surveillance	1	4.5%
Strict monitoring effect?	Improves safety	9	40.9%
	Encourages hiding behaviour	8	36.4%
	Depends on age/maturity	5	22.7%
AI rec ban for under-18?	Yes, completely	16	72.7%
Indian tech: Privacy by Design?	No profit over privacy	13	59.1%

Table 4: Legal Professional Assessment of DPDP Act and Platform Governance (n=22)

D. Finding 4: Age Circumvention and the Failure of Age-Gating

The student sub-cohort (n=84) generated perhaps the study's most striking empirical finding regarding the operational failure of age verification. When asked whether they had lied about their age to join a social media platform, 53.6% confirmed having done so 31.0% once or twice, and 22.6% many times.⁴² An additional 51.2% reported using VPNs, Incognito mode, or secondary 'private' accounts (Finstas) to bypass parental or age-based restrictions (34.5% occasionally; 16.7% frequently).⁴³

When asked whether the current age of digital majority (eighteen years) in India is too

high, 64.3% of students responded 'No 18 is appropriate for safety', while 26.2% believed it should be lowered to thirteen or sixteen.⁴⁴ This majority view that eighteen is appropriate for safety coexists with near-majority circumvention behaviour, revealing that adolescents conceptually accept safety restrictions while operationally bypassing them. This is a paradigmatic expression of the Privacy-Safety Paradox at the individual level.

The data on parental monitoring's psychological effects is also significant: 44.0% of students reported that parental monitoring caused feelings of anxiety or restricted freedom⁴⁵ a finding with

⁴² Survey data, Question 40 (n=84 students).

⁴³ Survey data, Question 42 (n=84).

⁴⁴ Survey data, Question 41 (n=84).

⁴⁵ Survey data, Question 43 (n=84).

constitutional resonance given that the right to privacy encompasses an individual's right to develop their personality and identity.

Lied about age on social media as minor	Yes (once or twice)	26	31.0%
	Yes (many times)	19	22.6%
	No, used real age	31	36.9%
	No, waited for legal age	8	9.5%
Used VPN/Incognito to bypass restrictions	Yes (occasionally)	29	34.5%
	Yes (frequently)	14	16.7%
	No (followed rules)	19	22.6%
	No (did not know how)	22	26.2%
18 years of digital majority: too high?	No 18 is appropriate for safety	54	64.3%
	Yes should be 13 or 16	22	26.2%
Parental monitoring caused anxiety/restriction	Yes	37	44.0%
	No	47	56.0%

Table 5: Student Circumvention Behaviour and Perceptions of Age Restriction (n=84)

E. Finding 5: Regulatory Architecture DPB Suo Motu Powers and Strict Liability for Algorithmic Harm

Among ed-tech and technology professionals (n=14), significant empirical support emerged for structural regulatory reforms targeting algorithmic harms. On whether the Data Protection Board should have suo motu powers to investigate harms caused to

children by predictive algorithms without a formal complaint, 59.1% of legal professionals scored this 4 or 5/5 (strong agreement).⁴⁶ In the tech cohort, 71.4% supported strict liability of technology companies for psychological harms caused by predictive algorithms in minors.⁴⁷

On breaking end-to-end encryption (E2EE) to identify Child Sexual Abuse Material

⁴⁶ Survey data, Question 23 (n=22 legal professionals, Scores 4/5 for DPB suo motu powers).

⁴⁷ Survey data, Question 35 (n=14 tech sub-cohort): 71.4% Yes for strict liability.

(CSAM), 71.4% of the technology sub-cohort considered this a 'reasonable restriction' on the right to privacy⁴⁸ Though this finding must be treated with caution given the small sub-cohort size (n=14) and the significant constitutional and technical debates this question engages. Among all respondents (n=157), 88.0% viewed the DPDP Act overall as a 'big step forward' for digital freedom, indicating a baseline institutional legitimacy for the legislative framework.⁴⁹

The primary protector of children's online safety was identified by 42.7% of all respondents as parents (individual responsibility), followed by technology companies (23.6%), the State (19.1%), and the child through self-regulation via education (14.6%).⁵⁰ This distribution underscores a critical governance insight: the dominant stakeholder perception locates protective responsibility primarily with parents, the same stakeholder group that the empirical data shows to have the lowest digital literacy and most fragmented protective behaviour.

DPB Suo Motu Powers (legal professionals, n=22)	Strong/Very Strong Agreement (45/5)	59.1%
Tech companies strictly liable for algo harms (tech cohort, n=14)	Yes support strict liability	71.4%
Breaking E2EE for CSAM = reasonable restriction (tech cohort, n=14)	Yes reasonable restriction	71.4%
DPDP Act overall = step forward (all, n=150)	Big step forward	88.0%
Primary protector of child online (all, n=157)	Parents (individual responsibility)	42.7%
	Tech Companies (platform design)	23.6%
	State (law & regulation)	19.1%
	Child (self-regulation via education)	14.6%

Table 6: Regulatory Architecture Preferences Key Empirical Indicators

⁴⁸ Survey data, Question 36 (n=14 tech sub-cohort): 71.4% Yes for E2EE break as reasonable restriction.

⁴⁹ Survey data, Question 50 (n=150): 88.0% 'Big Step Forward.'

⁵⁰ Survey data, Question 49 (n=157).

V. Constitutional and statutory framework

A. The Constitutional Architecture: Privacy, Dignity, and Children

The constitutional foundation for children's digital privacy in India is the nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India,⁵¹ wherein the Supreme Court unanimously recognised privacy as a fundamental right under Article 21. Chandrachud J. 's plurality opinion is particularly significant for children's privacy: it articulates privacy's three dimensions spatial, decisional, and informational and anchors informational privacy in the constitutional guarantee of personal liberty. The decision establishes that any State action impairing privacy must satisfy a three-pronged proportionality test: legality (existence of a law); legitimate aim; and proportionality in a strict sense.

The proportionality requirement is constitutionally decisive for the Privacy-Safety Paradox. Section 9's blanket parental consent requirement for all users under eighteen must satisfy this test. The legitimate aim (child protection) is uncontroversial. The proportionality question whether blanket parental consent for seventeen-year-olds is a proportionate means to that end when more calibrated alternatives (graduated age thresholds, mature minor assessments) exist is live and contested. The empirical finding that 45.5% of legal professionals view Section 9 as conflicting with the informational autonomy of mature minors

(16-18 years)⁵² directly reflects this constitutional anxiety.

B. The Digital Personal Data Protection Act, 2023: Architecture and Child-Protective Provisions

The DPDP Act represents India's first comprehensive data protection statute.⁵³ Its principal child-protective provision, Section 9, imposes three obligations on Data Fiduciaries: (i) to obtain verifiable consent of the parent or guardian before processing any personal data of a child (defined as anyone below eighteen years); (ii) to not process data in a manner likely to cause any detrimental effect on the wellbeing of the child; and (iii) to not undertake tracking or behavioral monitoring of children or targeted advertising directed at children. Section 10 designates certain Data Fiduciaries as 'Significant Data Fiduciaries', subjecting them to enhanced obligations including data protection impact assessments, data audits, and appointment of a Data Protection Officer.

The Act establishes the Data Protection Board of India (DPB) as the principal regulatory authority, with powers to investigate complaints, impose financial penalties (up to ₹250 crores per violation), and issue directions. However, the DPB has not yet become operationally effective as of June 2026, and the Rules contemplated under the Act essential for operationalising Section 9's age verification and consent mechanisms have not yet been finalised.⁵⁴

⁵¹ Justice K.S. Puttaswamy (Retd.) v Union of India (India) [hereinafter Puttaswamy], per D Y Chandrachud J (as he then was), discussing the requirement that any restriction on privacy must satisfy the tests of legality, legitimate State aim, and proportionality.

⁵² Survey data, Question 25 (n=22 legal professionals, Scores 45/5 = strong agreement that Section 9 conflicts with informational autonomy of 16-18 year olds). Specifically: 31.8% (Scores 45).

⁵³ DPDP Act, supra note 2, Schedule 1 (penalty provisions: up to INR 250 crores for certain categories of violation).

⁵⁴ Ministry of Electronics and Information Technology (India), Status Update on DPDP Rules Consultation (February 2026) (Rules consultation process ongoing; operationalisation of DPB pending). See also Internet

C. The Internal Tensions of Section 9

Section 9 contains three normative tensions that the empirical data illuminates. First, the ConsentMinimisation Tension: 41.1% of legal professionals rated the proposition that mandating 'verifiable parental consent' leads to excessive data collection (Aadhaar/IDs), violating the principle of data minimisation, at 4 or 5/5.⁵⁵ This is the Identification Paradox: requiring parents to produce identity documents for age verification purposes generates a privacy violation in service of privacy protection.

Second, the UniformityAutonomy Tension: 31.8% of legal professionals strongly agreed (45/5) that Section 9 conflicts with the right to informational autonomy of mature minors (16-18 years).⁵⁶ This is the Mature Minor Problem: the Act treats the digital consent question as binary when child development science and constitutional proportionality both demand a developmental spectrum.

Third, the RegulationCircumvention Tension: the empirical evidence that 53.6% of students have lied about their age online and 51.2% have used technical workarounds⁵⁷ demonstrates that the law's current deterrence architecture is demonstrably ineffective. Regulatory burdens that are routinely circumvented by the regulated population do not serve either privacy or safety.

VI. Comparative analysis: gdpr, uk aadc, and coppa

A. GDPR: The Gold Standard and Its Differential Age Architecture

The General Data Protection Regulation (EU) 2016/679 (GDPR)⁵⁸ establishes the international benchmark. Article 8 conditions processing of children's data on parental consent for users below sixteen years (with member states permitted to lower the threshold to thirteen). Crucially, Article 8's regime does not apply to users above the applicable threshold older teenagers engage the general GDPR framework on equal terms with adults. This graduated approach is fundamentally more consistent with child development principles and the mature minor doctrine than the DPDP Act's uniform eighteen-year threshold.

Article 22 GDPR establishes a right not to be subject to solely automated decisions producing significant effects, a direct algorithmic rights provision absent from the DPDP Act. Recital 38 mandates that child-specific advertising 'requires specific protection,' and the EDPB's Guidelines 3/2022⁵⁹ specifically identify and prohibit dark patterns in social media interfaces categories of manipulative design architecture that are not addressed anywhere in the DPDP Act.

Enforcement has been substantive: the Irish Data Protection Commission imposed a €345 million fine on TikTok in September 2023 for violations including unlawful processing of children's data, non-

Freedom Foundation, 'DPDP Rules: An Analysis of the Draft' (IFF Working Paper, March 2026).

⁵⁵ Survey data, Question 24 (n=22 legal professionals, Scores 45 combined = 41.1%; note: 4 = 18.2% and 5 = 22.7%).

⁵⁶ Survey data, Question 25 (n=22 legal professionals, Scores 45 = 31.8%).

⁵⁷ Survey data, Question 40 (n=84 students).

⁵⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1 [hereinafter GDPR], arts. 8, 22.

⁵⁹ European Data Protection Board, Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them (adopted 14 March 2023) [hereinafter EDPB Guidelines 3/2022].

transparent default settings, and inadequate age verification⁶⁰ the largest GDPR penalty relating to children's data.

B. UK Age Appropriate Design Code: The Child-Centred Design Standard

The UK Age Appropriate Design Code (Children's Code),⁴² operative from September 2021, is the world's most child-specific digital design regulation. Its fifteen standards include: Standard 4 (best interests of the child as primary design consideration); Standard 9 (no profiling of children for commercial purposes unless demonstrably in the child's best interest); Standard 11 (prohibition of nudge techniques encouraging children to provide unnecessary data); and Standard 15 (data protection impact assessments for services likely to be accessed by children). The Code is notable for applying to services 'likely to be accessed by children' rather than only services directed at children, a broader and more effective jurisdictional hook.⁶¹

The empirical data suggests strong alignment between Indian professional opinion and the UK AADC's approach: 72.7% of legal professionals support banning AI personalized recommendations for under-eighteens⁶² consistent with Standard 9 of the

Code. The ICO imposed a £12.7 million penalty on TikTok in April 2023 for violations of the Children's Code.⁶³

C. COPPA: The Foundational US Framework and Its Modernisation Challenge

The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 65016506, enacted in 1998 and revised in 2013,⁶⁴ establishes baseline protections for children under thirteen in the United States. COPPA's limitations are well-documented: its thirteen-year threshold protects only younger children; it does not address algorithmic recommendation systems; and its enforcement has been inconsistent. The FTC's record \$170 million penalty against Google/YouTube in 2019⁶⁵ demonstrated both the law's enforcement potential and its inadequacy for algorithmic-era challenges.

COPPA's modernisation trajectory COPPA 2.0 (S.1418, 118th Cong., 2023) and the Kids Online Safety Act (KOSA)⁶⁶ proposes extending protection to sixteen-year-olds and imposing a duty of care on platforms to protect minors from algorithmic harms, precisely the reforms this article recommends for India.

⁶⁰ Data Protection Commission (Ireland), Decision in Inquiry EN-21-2021 (TikTok Technology Limited), €345 million fine (September 15, 2023), available at <<https://www.dataprotection.ie/en/dpc-guidance/decisions>>.

⁶¹ UK AADC, supra note 42, s. 1 (scope: 'information society services likely to be accessed by children').

⁶² Survey data, Question 27 (n=22).³⁸

⁶³ Information Commissioner's Office (UK), Press Release, 'TikTok Fined £12.7m for Misusing Children's Data' (April 4, 2023) <<https://ico.org.uk>>.

⁶⁴ Children's Online Privacy Protection Act, 15 U.S.C. §§ 65016506 (1998, amended 2013) [hereinafter COPPA].

⁶⁵ United States v. Google LLC and YouTube, LLC, Complaint, No. 1:19-cv-02642 (D.D.C. filed September 4, 2019); FTC Press Release, 'Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law' (September 4, 2019).

⁶⁶ Children and Teens Online Privacy Protection Act, S. 1418, 118th Cong. (2023) [COPPA 2.0]; Kids Online Safety Act, S. 1409, 118th Cong. (2023) [KOSA].

D. Comparative Regulatory Assessment Table

Parameter	DPDP Act 2023(India)	GDPR(EU)	UK AADC	COPPA(US)
Child age threshold	Under 18 (blanket)	Under 16/13 (graduated)	Under 18 (design-led)	Under 13
Mature minor recognition	None	Partial (1316 self-consent)	Implicit (evolving capacities)	None
Behavioral profiling ban	Section 9(3) vague	Art. 22 automated decisions	Standard 9 explicit ban	Not addressed
Algorithmic transparency	Not required	Art. 22 right to explanation	Standard 14 required	Not required
Dark patterns prohibition	Not addressed	EDPB GL 3/2022	Standard 11 explicit	Not addressed
Privacy by default	Not specified	Art. 25 (Privacy by Design)	Standard 7 required	Opt-in collection
Age verification standards	Not specified	Proportionate measures	ICO Age Assurance Standard	Reasonable measures
Enforcement body	DPB (non-operational)	National DPAs (active)	ICO (active)	FTC (active)
Recent major penalty	None yet	TikTok €345M (2023)	TikTok £12.7M (2023)	Google \$170M (2019)
Algorithmic impact assessment	Not mandated	Art. 35 DPIA	Standard 15 required	Not required

Table 7: Comparative Regulatory Framework Assessment**VII. Critical Analysis: The DPDP Act Against Empirical Reality****A. The Consent Architecture: Empirically Validated Inadequacy**

The DPDP Act's reliance on parental consent as the primary protective mechanism for children is empirically undermined by the data in three independent ways. First, 48.6% of parents are

unaware of the Act's own provisions.⁶⁷ Second, 51.3% rarely or never check privacy settings on their child's devices.⁶⁸ Third, over 50% of their children bypass age restrictions through technical circumvention.⁶⁹ A consent regime in which the consenting party lacks digital literacy, the regulated subject circumvents the consent mechanism, and the regulatory body is non-operational is a consent regime that does not protect children. The parallel risk that robust consent mechanisms generate their own privacy violations through identity data collection is reflected in the finding that 45.9% of parents would delete an app rather than permit Aadhaar-based age verification.⁴⁸ This resistance captures the Identification Paradox at the individual level: the very mechanism designed to protect children (age verification via Aadhaar) is itself perceived as a privacy violation by nearly half the parent cohort.

B. The Algorithmic Governance Gap: The Central Deficiency

The DPDP Act's most significant deficiency in light of both the empirical data and the comparative analysis is the absence of specific algorithmic governance provisions. Section 9(3) vaguely prohibits processing 'likely to cause detrimental effects on wellbeing' but provides no definition of algorithmic profiling, no prohibition on recommendation system optimization for child engagement, no requirement for algorithmic impact assessments, and no right to explanation for automated decisions affecting children. This gap is constitutionally problematic: the right to informational privacy under Puttaswamy necessarily encompasses a right not

to be subjected to manipulative algorithmic architecture that exploits children's developmental vulnerabilities without meaningful disclosure or consent.⁷⁰ The empirical data confirms strong professional support for closing this gap: 59.1% of legal professionals support suo motu DPB powers to investigate algorithmic harms⁷¹; 71.4% of tech professionals support strict platform liability for algorithmic psychological harms⁷²; and 72.7% support banning AI-personalised recommendations for under-eighteens.⁷³

C. The Age Uniformity Problem: Constitutional Vulnerability

The DPDP Act's eighteen-year threshold for parental consent is constitutionally vulnerable to challenge under the proportionality standard articulated in Puttaswamy.⁷⁴ As the empirical data shows, 45.5% of legal professionals view Section 9 as conflicting with the informational autonomy of mature minors aged sixteen to eighteen.⁷⁵ A law that applies parental consent requirements to university-aged adults (seventeen-to-eighteen-year-olds) for activities as ordinary as creating a social media profile may be challenged as failing the proportionality test's third prong: whether less restrictive alternatives are available (e.g., a graduated threshold of thirteen, fifteen, and eighteen years with corresponding graduated safeguards).

D. Enforcement Architecture: The Operational Void

The Data Protection Board's non-operational status more than two years after the Act's enactment represents a critical systemic failure.⁷⁶

⁶⁷ Survey data, Question 8 (n=37 parents/guardians). Note: The question appeared to route primarily to parents; the 37 responding to this item are treated as the parental sub-cohort throughout.

⁶⁸ Survey data, Question 9 (n=37).

⁶⁹ Survey data, Question 40 (n=84 students).

⁷⁰ United Nations Children's Fund, Policy Guidance on AI for Children (2021); Gerison Lansdown, The Evolving Capacities of the Child (United Nations Children's Fund and Save the Children Innocenti Research Centre 2005).

⁷¹ Survey data, Question 23 (n=22 legal professionals, Scores 45/5 for DPB suo motu powers).

⁷² Survey data, Question 35 (n=14 tech sub-cohort): 71.4% Yes for strict liability.

⁷³ Survey data, Question 27 (n=22).³⁸

⁷⁴ Chandrachud J. held that any restriction on the fundamental right to privacy must satisfy the requirements of legality, a legitimate State aim, and proportionality.

⁷⁵ Survey data, Question 25 (n=22 legal professionals, Scores 45/5 = strong agreement that Section 9 conflicts with informational autonomy of 16-18 year olds). Specifically: 31.8% (Scores 45).

⁷⁶ Ministry of Electronics and Information Technology (India), Status Update on DPDP Rules Consultation (February 2026) (Rules consultation

In comparative perspective, active enforcement has been essential to the effectiveness of both GDPR (Irish DPC's €345M TikTok fine) and the UK AADC (ICO's £12.7M TikTok fine). The absence of an operationally effective DPB means that the DPDP Act's child-protective provisions exist as a normative aspiration rather than a functioning regulatory instrument, a condition that directly exposes Indian children to ongoing algorithmic privacy violations without effective legal redress.

VIII. Emerging challenges in children's digital privacy

A. The AI Learning Surveillance Paradox

The empirical data illuminates a specific emerging challenge with particular clarity: the AI learning surveillance paradox. When asked about an AI-based learning app that tracks children's eye movements and facial expressions via camera to detect boredom and adjust lessons, claiming a 40% improvement in learning outcomes, respondents across all cohorts were divided between the educational benefit and the biometric privacy intrusion.⁷⁷ This scenario crystallises the Privacy-Safety Paradox in the ed-tech domain: the tracking mechanism that promises educational benefit requires biometric surveillance of a child that most data protection frameworks would class as sensitive personal data requiring explicit, specific consent.

The DPDP Act does not distinguish biometric data as a special category requiring heightened protection, a significant gap compared to GDPR Article 9, which classifies biometric data processed for identification purposes as a special category subject to prohibition save for specific exceptions.⁷⁸

process ongoing; operationalisation of DPB pending). See also Internet Freedom Foundation, 'DPDP Rules: An Analysis of the Draft' (IFF Working Paper, March 2026).

⁷⁷ Survey data, Question 51 (n=157, qualitative/mixed responses on AI eye-tracking learning app scenario).

⁷⁸ GDPR, supra note 39, art. 9 (special categories of personal data: biometric data processed for identification purposes prohibited save for specified exceptions).

B. The 'Regulation-to-Unsafe-Platforms' Migration Risk

A particularly significant empirical finding with direct regulatory design implications is the near-majority view among legal professionals that strict regulations on mainstream platforms (Instagram, YouTube) will push children toward hidden or less-safe platforms (68.2% rating this likelihood at 4 or 5/5).⁷⁹ This is the 'Displacement Effect' risk: poorly designed age-gating or platform restrictions on major platforms with substantial institutional safety infrastructure may displace child users to unregulated alternatives with far greater harm potential. This risk argues strongly for a regulatory design approach that focuses on behavioural standards applicable across all platforms (as under the UK AADC) rather than platform-specific prohibitions.

C. Cross-Border Data Flows and Jurisdictional Limitations

The personal data of Indian children processed by Meta (US), Google (US), ByteDance (China), and other non-Indian platforms is routinely transferred across jurisdictions. Section 16 of the DPDP Act grants the Central Government broad discretion to designate restricted jurisdictions for data transfers, but this provision has not yet been operationalised.⁸⁰ The practical result is that Indian children's behavioral data is currently processed in foreign jurisdictions under foreign legal regimes that may provide less protection than the DPDP Act's own standards.

D. Metaverse, Extended Reality, and the Next Frontier

Metaverse and extended reality (XR) technologies which collect unprecedented

⁷⁹ Survey data, Question 22 (n=22 legal professionals, Scores 45: 68.2% 'Yes, strict regulations push children to unsafe platforms').

⁸⁰ DPDP Act, supra note 2, § 16 (cross-border data transfers); Ministry of Electronics and Information Technology, DPDP Rules Status, supra note 36 (§ 16 not yet operationalised).

volumes of biometric, physiological, and behavioral data including gaze tracking, body movement, and emotional signals represent the next generation of child privacy challenges.⁸¹ Neither the DPDP Act nor any other current Indian statute addresses these technologies specifically. The Act's broad definition of 'personal data' would technically encompass XR-generated data, but the absence of specific restrictions on its processing for child users represents a significant prospective gap.

Ix. Recommendations

On the basis of the doctrinal analysis, comparative assessment, and empirical findings, this article advances seven calibrated legislative and policy recommendations:

Recommendation 1: Graduated Digital Consent Architecture

India should replace the DPDP Act's uniform eighteen-year threshold with a three-tier graduated consent architecture: (i) Under 13: mandatory verifiable parental consent with data minimisation obligations and no behavioural tracking; (ii) 13-15: parental consent required for sensitive data processing and behavioral tracking but not for general platform access; (iii) 16-17: self-consent with heightened platform disclosure obligations. This architecture aligns with the 'evolving capacities' principle of UNCRC Article 5, resolves the constitutional proportionality concern regarding uniform parental consent for mature minors, and reduces the incentive for age circumvention by providing a legitimate pathway for older teenagers.⁸²

Recommendation 2: Mandatory Algorithmic Impact Assessments for Child Users

All Significant Data Fiduciaries operating platforms with significant child user bases should

be required to conduct and submit to the DPB a Children's Algorithmic Impact Assessment (CAIA) before deploying new algorithmic features. The CAIA should specifically assess: (i) the objectives for which recommendation algorithms are optimised; (ii) the behavioral data inputs; (iii) foreseeable risks to child wellbeing, including content escalation risks and psychological manipulation risks; and (iv) the safeguards implemented. This recommendation is empirically supported by 59.1% of legal professionals favouring suo motu DPB investigative powers over algorithmic harms.⁸³

Recommendation 3: Explicit Prohibition of Behavioural Advertising Directed at Minors

Section 9 of the DPDP Act should be amended to include an explicit prohibition on behavioural advertising directed at any user under eighteen years of age. Contextual advertising which does not require behavioural profiling should be permitted as a proportionate alternative. This reform is consistent with the UK AADC Standard 9, proposed COPPA 2.0 amendments, and GDPR Recital 38. Its empirical support is reflected in the 72.7% of legal professionals supporting an outright ban on AI-personalised recommendations for under-eight teens.⁸⁴

Recommendation 4: Establishment of a Children's Digital Rights Authority

A dedicated Children's Digital Rights Authority (CDRA) should be established, either as a statutory body or as a specialist division within the DPB with operational independence. The CDRA should be vested with: (i) suo motu investigative powers over algorithmic harms to children; (ii) power to issue platform-specific design standards under a statutory best interests of the child framework; (iii) power to receive complaints from children and guardians; and (iv) power to commission independent algorithmic

⁸¹ European Parliament, Resolution on Artificial Intelligence in Education, Culture and the Audiovisual Sector, 2020/2017(INI) (2020); Jon Radoff, 'The Metaverse and Web3' Forbes Technology Council (2022).

⁸² cf. UK AADC, supra note 42 (applies to services 'likely to be accessed by children' under 18, with proportionate measures); GDPR, supra note 39, art. 8 (graduated age threshold).

⁸³ Survey data, Question 23 (n=22 legal professionals, Scores 45/5 for DPB suo motu powers).

⁸⁴ Survey data, Question 27 (n=22).

audits. This recommendation is directly grounded in the empirical finding that 59.1% of legal professionals strongly support DPB suo motu powers over algorithmic child harms.⁸⁵

Recommendation 5: Technical Age Assurance Standards

The DPB should issue technical standards for age assurance, drawing on the UK ICO's Age Assurance Technical Report and the Information Commissioner's evidence-based framework for proportionate age verification methods. Platforms should be required to implement proportionate age assurance before enabling behavioral tracking or content recommendation for child users. The empirical finding that 45.9% of parents would delete apps requiring Aadhaar-based age verification⁸⁶ argues for a plurality of age assurance methods to avoid Aadhaar-dependency as a single verification pathway.

Recommendation 6: Digital Literacy as Structural Protective Infrastructure

Given the empirical finding that parental technical literacy is identified as the single largest barrier to effective digital child safety (78.6% of tech sub-cohort rating at 45/5),⁸⁷ and that only 47.5% of students reported receiving any formal digital citizenship or data rights education, structured digital literacy programmes should be mandated as part of the school curriculum under the National Education Policy 2020 framework. Platform obligations to provide accessible privacy dashboards for parents and guardians should be legislated under the DPDP Rules.

Recommendation 7: Strict Liability Framework for Algorithmic Psychological Harms

Technology companies should be subjected to a regime of strict liability for proven psychological harms like addiction, depression, anxiety, self-

harm ideation, causally attributable to their predictive algorithms in users under eighteen years. The evidential burden should require plaintiffs to establish causation through algorithmic audit evidence, shifting the burden to the platform to demonstrate that its algorithmic architecture operated within safety standards. The empirical endorsement of this approach by 71.4% of technology professionals⁸⁸ reflects the professional community's recognition that the current liability framework is inadequate to deter algorithmic harm.

X. CONCLUSION

The Privacy-Safety Paradox: the structural tension between children's safety and children's privacy in digital governance is not merely an academic construct. It is an empirically validated reality in the lives of Indian children, parents, legal professionals, and technology educators. The 157 respondents surveyed in this study do not merely illustrate the paradox; they embody it: parents who prioritise safety but distrust the platforms charged with delivering it; teenagers who conceptually accept age restrictions but routinely circumvent them; legal professionals who believe the DPDP Act is simultaneously insufficient for child safety and insufficiently protective of child autonomy; technologists who support strict platform liability while recognising that total tracking bans would impair educational tools.

The DPDP Act, 2023 is an important legislative milestone, and the 88.0% of respondents who view it as a step forward for digital freedom are not wrong to do so. But the Act's child-protective provisions as this study demonstrates through the convergent lens of doctrinal analysis, comparative law, and empirical evidence are structurally inadequate for the algorithmic age in four decisive respects: the consent regime is

⁸⁵ Survey data, Question 23 (n=22 legal professionals, Scores 45/5 for DPB suo motu powers).

⁸⁶ Survey data, Question 14 (n=37 parents): 45.9% would delete apps to protect privacy.

⁸⁷ Survey data, Question 32 (n=14 tech sub-cohort, Scores 45 = 78.6% for parental technical literacy as biggest hurdle).

⁸⁸ Survey data, Question 35 (n=14 tech sub-cohort): 71.4% Yes for strict liability.

operationally circumvented by children and lacks parental digital literacy infrastructure to function; the age uniformity of eighteen years is constitutionally disproportionate and developmentally irrational; the Act contains no specific algorithmic governance provisions despite algorithmic profiling being the primary mechanism of children's privacy violation; and the enforcement body remains non-operational.

The reforms proposed in this article a graduated digital consent architecture, mandatory algorithmic impact assessments, prohibition of behavioural advertising directed at minors, a Children's Digital Rights Authority with suo motu powers, technical age assurance standards,

digital literacy as structural infrastructure, and strict platform liability for algorithmic psychological harms constitute a coherent, evidence-based legislative programme that resolves the Privacy-Safety Paradox not by choosing one value over the other, but by designing a regulatory architecture sophisticated enough to protect both.

India's constitutional framework, its obligations under the UNCRC, and the lived digital experience of its youngest citizens demand nothing less. The Privacy-Safety Paradox is not a problem to be managed; it is a challenge to be transcended through law.

BIBLIOGRAPHY

A. Table of Cases

- Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
 Shafin Jahan v Asokan KM (2018) 16 SCC 368.
 Independent Thought v Union of India (2017) 10 SCC 800.
 Gillick v West Norfolk and Wisbech Area Health Authority [1986] AC 112 (HL).
 United States v Google LLC and YouTube, LLC, Complaint, No. 1:19-cv-02642 (D.D.C. filed 4 September 2019).

B. Table of Legislation and Regulatory Instruments

- Constitution of India, arts 14, 15(3), 21 and 21A.
 Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
 Ministry of Electronics and Information Technology (India), Draft Digital Personal Data Protection Rules, 2025.
 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1.
 Data Protection Act 2018 (UK) and the Age Appropriate Design Code (Information Commissioner's Office, UK).
 Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998, amended 2013).
 Children and Teens' Online Privacy Protection Act, S. 1418, 118th Cong. (2023) [COPPA 2.0].
 Kids Online Safety Act, S. 1409, 118th Cong. (2023) [KOSA].
 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).
 United Nations Children's Fund, *Policy Guidance on AI for Children* (2021).
 European Union, *General Data Protection Regulation*, recitals 38 and 58; arts 8 and 25.
 Organisation for Economic Co-operation and Development, *Recommendation of the Council on Children in the Digital Environment* (2021).

C. International Instruments

- United Nations, *Convention on the Rights of the Child*, 20 November 1989, 1577 UNTS 3.
 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc CRC/C/GC/25 (2 March 2021).
 OECD, *Recommendation of the Council on Children in the Digital Environment* (2021).
 European Parliament, *Resolution on Artificial Intelligence in Education, Culture and the Audiovisual Sector*, 2020/2017(INI) (2020).

D. Books and Book Chapters

- Sonia Livingstone and Alicia Blum-Ross, *Parenting for a Digital Future: How Hopes and Fears About Technology Shape Children's Lives* (Oxford University Press 2020).
 Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (HarperCollins India 2018).
 Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2021).
 Aparna Chandra and others, *The Indian Data Protection Landscape* (Oxford University Press 2023).
 Gerison Lansdown, *The Evolving Capacities of the Child* (UNICEF and Save the Children Innocenti Research Centre 2005).
 Norman K Denzin, *The Research Act: A Theoretical Introduction to Sociological Methods* (Transaction Publishers 2009).
 John W Creswell and J David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th edn, Sage 2018).
 Beeban Kidron, 'Children's Digital Rights and the Value of Data' in Jonathan Todres and Shani M King (eds), *The Oxford Handbook of Children's Rights Law* (Oxford University Press 2020) 387.

E. Journal Articles

- Sonia Livingstone, 'Children: A Special Case for Privacy?' (2018) 39 *Intermedia* 14.

Usha Ramanathan, 'Privacy and the Aadhaar System' (2017) 52 Economic and Political Weekly 77.
 Arindrajit Basu and Elonnai Hickok, 'The Risks of Surveillance' (2019) Centre for Internet and Society Working Paper.

Nishtha Jaswal, 'Informational Autonomy and the Mature Minor: Implications for Data Protection Law in India' (2024) 6 Indian Journal of Law and Technology 112.

F. Reports and Official Documents

UNICEF, The State of the World's Children 2017: Children in a Digital World (UNICEF 2017).

UNICEF, The State of the World's Children 2021: On My Mind (UNICEF 2021).

UNICEF, Policy Guidance on AI for Children (2021).

UNESCO, Education in a Post-COVID World: Nine Ideas for Public Action (2020).

OECD, Going Digital: Shaping Policies, Improving Lives (OECD Publishing 2019).

Statista, Number of Internet Users in India from 2015 to 2028 (2024).

United Nations Population Fund (UNFPA), State of World Population 2023 (2023).

Internet Freedom Foundation, Analysing the Digital Personal Data Protection Act, 2023 (2023).

Internet Freedom Foundation, 'DPDP Rules: An Analysis of the Draft' (IFF Working Paper, March 2026).

Ministry of Electronics and Information Technology (India), Status Update on DPDP Rules Consultation (February 2026).

European Data Protection Board, Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them (adopted 14 March 2023).

Data Protection Commission (Ireland), Decision in Inquiry EN-21-2021 (TikTok Technology Limited) (15 September 2023).

Information Commissioner's Office (UK), Press Release, 'TikTok Fined £12.7m for Misusing Children's Data' (4 April 2023).

Federal Trade Commission, Press Release, 'Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law' (4 September 2019).

Jon Radoff, 'The Metaverse and Web3' Forbes Technology Council (2022).

G. Primary Data

Author's empirical survey conducted between January and April 2026, comprising 157 respondents across 13 Indian States, including sub-cohorts of parents/guardians (n=37), students (n=84), legal professionals (n=22), and technology-sector respondents (n=14) (survey data on file with the author).