INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 4 | 2026 Art. 07

Children's Privacy on Social Media Platforms in India: Examining the Adequacy of the Digital Personal Data Protection Act, 2023

Divakar
Law Student, 4th Year, BA.LL.B.,
Bharati Vidyapeeth New Law College Pune

Recommended Citation
Divakar, *Children's Privacy on Social Media Platforms in India: Examining the Adequacy of the Digital Personal Data Protection Act, 2023,* 5 IJHRLR 82-94 (2026).
Available at www.ijhrlr.in/current-issues/.

Children's Privacy on Social Media Platforms in India: Examining the Adequacy of the Digital Personal Data Protection Act, 2023

ABSTRACT

The proliferation of social media platforms in India has created unprecedented challenges for children's privacy protection, with millions of minors exposed to comprehensive data collection, behavioral profiling, and algorithmic manipulation. The Digital Personal Data Protection Act (DPDPA), 2023, represents India's first comprehensive statutory response to digital privacy concerns. However, this article argues that while the DPDPA establishes important foundational protections, structural ambiguities within its children's privacy framework introduce distinct operational frictions. Through a critical analysis of the Act's provisions specific to the Indian context, an examination of pre-existing Indian legal frameworks, and an assessment against documented harms affecting Indian children, this article evaluates key regulatory pain points. While the statutory text of the DPDPA actively prohibits targeted advertising, behavioral tracking, and nominal child consent through a strict, baseline age threshold of eighteen under Section 2(f) and Section 9, significant policy gaps remain unaddressed. Chief among these is the enforcement of a rigid, blanket age gate that ignores the legal doctrine of evolving capacities, leaving a vulnerable gray area regarding organic engagement-maximizing algorithms that manipulate minor psychology without technically crossing into banned targeted marketing. Furthermore, the article analyzes the upcoming framework of the Digital Personal Data Protection Rules, evaluating how this imminent secondary legislation will shift the immediate challenge from regulatory absence to practical, systemic implementation and enforcement by the proposed Data Protection Board of India (DPBI). The article concludes that legislative amendments establishing explicit, tiered child-centric protections tailored to India's unique developmental and socio-cultural context paired with structural mandates for automated Data Protection Impact Assessments (DPIAs) and direct administrative coordination with national child welfare bodies are essential to adequately insulate Indian children within contemporary digital environments.

KEYWORDS

Digital Personal Data Protection Act (DPDPA) 2023, Children's Digital Privacy, Social Media Platforms, Algorithmic Profiling,

Verifiable Parental Consent, Data Fiduciary, Target Advertising Ban, Data Protection Board of India (DPBI), Evolving Capacities, Child Welfare Laws.

INTRODUCTION

India's digital revolution has fundamentally reconfigured the socio-technological landscape, positioning social media platforms as ubiquitous infrastructure in the daily lives of millions of minors. According to data from the Internet and Mobile Association of India (IAMAI), India's digital user base has expanded exponentially, with children and adolescents constituting an increasingly critical demographic across platforms such as Meta (Facebook and Instagram), YouTube, WhatsApp, and Snapchat.[1] While these digital ecosystems offer unprecedented avenues for pedagogical access, creative expression, and social democratization particularly by bridge-linking rural or marginalized Indian youth to previously inaccessible educational resources they simultaneously subject a deeply vulnerable demographic to systemic privacy risks. These risks manifest through pervasive data harvesting, sophisticated behavioral profiling, engagement-maximizing algorithms designed without developmental guardrails, and commercial monetization via hyper-targeted advertising.[2]

The gravity of these risks is compounded by India's unique socio-economic and digital landscape. A substantial segment of the minor population hails from first-generation digital households characterized by low digital literacy, creating a compounding vulnerability distinct from industrialized nations where digital safety architectures are more mature. This vulnerability is not merely structural but deeply cognitive. Neurodevelopmental research establishes that the prefrontal cortex the locus of executive functioning, risk mitigation, and long-term consequence assessment continues maturation well into an individual's mid-twenties.[3] Consequently, minors inherently lack the developmental capacity to fully comprehend the downstream ramifications of immediate online disclosures. Empirical studies within the Indian context corroborate that even technologically adept children struggle to decipher the labyrinthine trajectories of multi-intermediary data flows, the opacity of algorithmic decision-making, and the secondary commercial repurposing of their personal data within the domestic digital marketplace. This cognitive asymmetry, weaponized by the

[1] Internet and Mobile Association of India (IAMAI) & Kantar, *Internet in India Report 2023* (2023).
[2] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8–10 (PublicAffairs 2019)
[3] Laurence Steinberg, A Social Neuroscience Perspective on Adolescent Risk-Taking, 28 Dev. Rev. 78 (2008).

predatory design architectures of social media platforms, nullifies the classic doctrine of "informed consent" for children.

Recognizing these systemic failures, the Parliament of India enacted the Digital Personal Data Protection Act, 2023 (DPDPA) on August 11, 2023, marking a paradigm shift in the nation's sovereign data governance strategy.[4] Designed as a native statutory framework rather than a derivative replication of foreign models like the European Union's General Data Protection Regulation (GDPR), the DPDPA sought to overhaul the historically fragmented, obsolete, and sector-specific privacy regime previously anchored under Section 43A of the Information Technology Act, 2000, and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[5]

However, deep analytical fissures persist regarding whether the DPDPA's structural architecture particularly Section 9, which governs the processing of personal data of children is sufficient to insulate minors from the predatory realities of the attention economy. The statutory choice to relegate the operational mechanics of child protection to delegated legislation (rules to be notified by the Central Government) and enforcement by the forthcoming Data Protection Board of India (DPBI) raises critical questions of adequacy, administrative delay, and enforcement efficacy.

THE LANDSCAPE OF CHILDREN'S PRIVACY IN INDIA'S DIGITAL ECOSYSTEM

Digital privacy within the Indian socio-legal context essentially encapsulates an individual's right to exercise informational self-determination, which means having the autonomy to control one's digital identity, regulate what personal information is disclosed and to whom, and protect against unauthorized surveillance and commercial exploitation. This concept attains profound constitutional weight in India following the Supreme Court's landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, which firmly established the right to privacy as a fundamental right under Article 21 of the Constitution.[6] For minor data subjects, this constitutional guarantee acquires a heightened, protective dimension due to distinct neurodevelopmental realities and structural vulnerabilities that separate children from adult data subjects, compounded by India's specific landscape where hyper-accelerated digital penetration has outpaced the development of comprehensive,

[4] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (Aug. 11, 2023).
[5] Information Technology Act, No. 21 of 2000, § 43A (India).
[6] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

child-centric regulatory safeguards. Seizing upon this techno-legal gap, global social media platforms operating in India deploy highly sophisticated data collection ecosystems that extend far beyond the information users consciously or voluntarily disclose, deliberately tailoring their data harvesting mechanisms to maximize information extraction from the nation's uniquely young, digitally enthusiastic population. This data collection apparatus operates aggressively across a continuous tripartite matrix of explicit, implicit, and inferred data points.

Explicit data encompasses information that Indian children actively provide, such as usernames, registration metrics, telephone numbers, user-generated images or videos, and direct peer-to-peer communications, where platforms frequently weaponize deceptive choice architectures or dark patterns to exploit minor psychological vulnerabilities and compel extensive profile completion through social design loops. Implicit data is harvested continuously and passively through automated tracking technologies operating entirely beneath the conscious awareness of the child, capturing behavioral metrics such as precise dwell time on specific content, search queries, location logs via GPS coordinates and cellular tower triangulation, and device-level diagnostics common to India's budget-hardware market, alongside biometric metadata extracted from uploaded content through facial and voice analysis. Representing the absolute apex of corporate data extraction, inferred data utilizes machine learning algorithms to analyze the convergence of these explicit and implicit data streams, constructing highly sensitive psychometric and behavioral dossiers that determine a child's personality traits, political leanings, religious beliefs (exceptionally volatile within India's pluralistic fabric), and specific psychological vulnerabilities. Empirical data underscores the staggering granularity of this surveillance, documenting that an average child user's profile on major social media platforms comprises thousands of discrete data points accumulated within a single year, generating comprehensive digital dossiers with a level of precision that far exceeds what Indian parents, educators, or even the children themselves possess regarding their own lives.

The monetization and algorithmic weaponization of these digital dossiers generate highly distinct pathways of systemic harm that are intimately shaped by Indian socio-cultural and economic dynamics. First, platforms exploit deep-seated cultural anxieties regarding academic achievement and socio-economic mobility, triggering an onslaught of predatory targeted advertisements for hyper-competitive coaching institutes, skill-development services, or appearance-altering products adapted to discriminatory beauty standards. Second, machine

learning architectures utilize variable reward schedules, infinite scroll mechanics, and the algorithmic prioritization of emotionally volatile content to maximize user attention, establishing compulsive usage patterns that research strongly correlates with clinical anxiety, depression, and severe sleep disruption. Third, the availability of these behavioral dossiers presents an acute child-welfare and security risk, as bad actors or trafficking networks can exploit behavioral markers to pinpoint vulnerable minors experiencing familial conflict or social isolation, subsequently tailoring grooming strategies to exploit those precise emotional fractures within specific Indian cultural contexts. Finally, because digital information is effectively permanent, data extracted from a vulnerable child persists indefinitely into adulthood, creating an irreversible digital footprint that can be weaponized in later years to influence creditworthiness evaluations within India's emerging digital credit systems, shape employment background checks, or facilitate systemic discrimination and exploitation throughout their adult life.

THE PRE-DPDPA LEGAL FRAMEWORK AND ITS INADEQUACIES IN INDIA

Prior to the enactment of the Digital Personal Data Protection Act (DPDPA), 2023, India's privacy protections evolved through a highly fragmented, sector-specific regime that fundamentally lacked the comprehensive scope or specialized statutory architecture required to protect minors in the digital attention economy. This framework developed across disparate constitutional and statutory spaces, none of which anticipated contemporary big-data extraction or the unique behavioral profiling of children. On the constitutional level, the Supreme Court of India delivered a monumental paradigm shift in *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*, ruling that the right to privacy is an indispensable, intrinsic facet of the right to life and personal liberty guaranteed under Article 21, thereby providing foundational constitutional protection to all natural persons, including children.[7] However, a critical limitation of this constitutional jurisprudence in practical application is that fundamental rights under the Indian Constitution are primarily enforceable vertically against state action under Article 12, leaving them largely inadequate for addressing horizontal privacy violations perpetrated by private transnational social media conglomerates. On the statutory plane, the Information Technology (IT) Act, 2000 enacted before the inception of modern social media and only partially updated via the Information Technology (Amendment) Act, 2008—served as India's primary text for digital regulation, containing structural deficiencies that rendered it obsolete for

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

minor protection. Specifically, Section 43A of the IT Act established a civil remedy by imposing corporate liability for compensation if negligence in maintaining "reasonable security practices" resulted in the unauthorized access, disclosure, or loss of "sensitive personal data or information" (SPDI).[8] However, Section 43A was severely restricted by its narrow, exhaustive definition of SPDI under the accompanying Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which limited protection strictly to structured datasets like financial data, health metrics, biometrics, and passwords.[9] Consequently, the vast matrices of implicit, behavioral, telemetry, and location data harvested continuously by social media platforms which represent the most commercially valuable and psychologically invasive categories of minor data remained outside the statutory definition of "sensitive" data. Furthermore, Section 43A operated as a reactive, tortuous mechanism requiring the affected party to establish clear proof of corporate negligence and actual, quantifiable "wrongful loss or wrongful gain," imposing an insurmountable evidentiary burden on minor data subjects and their guardians, while completely lacking any proactive, preventative regulatory oversight or ongoing compliance audits.

Similarly, the IT (SPDI) Rules, 2011, proved entirely ineffective as a child-protective architecture. While they mandated basic privacy policies and formal consent for data collection, they allowed corporate compliance to be satisfied through token contractual disclosures and dense, boilerplate privacy agreements that children could not comprehend. More importantly, these rules were completely blind to the systemic structural operations of modern social media platforms, providing no restrictions on algorithmic manipulation, automated behavioral tracking, or hyper-targeted advertising, nor did they provide any enforcement mechanisms beyond a fragmented, inaccessible complaints process to adjudicating officers under the Department of Telecommunications. While the Consumer Protection Act, 2019, subsequently introduced an alternative consumer dispute redressal mechanism by classifying deceptive data collection as an "unfair trade practice," its litigation-heavy, retrospective structure focused strictly on commercial consumer transactions rather than the systemic, non-monetary harms of minor data profiling.[10]Finally, India's existing specialized children's welfare statutes, namely the

[8] Information Technology Act, No. 21 of 2000, § 43A (India).
[9] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3, G.S.R. 313(E), Gazette of India, Extraordinary, Part II, Section 3(i) (Apr. 11, 2011).
[10] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3, G.S.R. 313(E), Gazette of India, Extraordinary, Part II, Section 3(i) (Apr. 11, 2011).

Juvenile Justice (Care and Protection of Children) Act, 2015, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, while robust in their respective operational spheres, were structurally engineered to penalize overt, physical, or explicit criminal exploitation and physical abuse.[11] They were completely disconnected from the underlying data processing pipelines, algorithmic feedback loops, and invisible surveillance architectures that actually facilitate and exacerbate these digital harms. This regulatory vacuum allowed social media platforms to operate within the Indian digital market with near-absolute immunity, establishing the unrestrained data extraction practices that continue to fuel the psychological, commercial, and predatory exploitation of millions of Indian children.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: INDIA'S COMPREHENSIVE RESPONSE

The enactment of the Digital Personal Data Protection Act (DPDPA), 2023, marks a definitive shift in sovereign data governance, establishing India's first unified, comprehensive legislative text designed to regulate the processing of digital personal data. Codifying key data protection principles including lawfulness, purpose limitation, data minimization, accuracy, storage limitation, and transparency the Act grants data principals unprecedented statutory rights to access, correction, erasure, and grievance redressal.[12] However, a critical analytical evaluation of its structural architecture reveals that the general definitions and child-specific protections contain acute systemic vulnerabilities. Specifically, Section 2(t) defines personal data as any data about an individual who is identifiable by or in relation to such data, but the framework explicitly excludes anonymized data from its ambit.[13] This creates a severe regulatory blind spot within India's emerging data economy, where supposedly anonymized data can be reverse-engineered and re-identified through algorithmic compilation and cross-referencing with secondary domestic datasets.

Furthermore, a significant doctrinal error often arises in premature critiques of the Act's child-protection mechanisms: contrary to early assumptions that the statute completely delegates child safety to future executive rulemaking under a generic clause, the DPDPA actually anchors its child-protective architecture in the strict statutory mandates of Section 9.[14] Section 2(f)

establishes a conservative, blanket threshold by defining a "child" as any

[11] Protection of Children from Sexual Offences Act, No. 32 of 2012 (India).
[12] Digital Personal Data Protection Act, No. 22 of 2023, ch. III (India).
[13] Digital Personal Data Protection Act, No. 22 of 2023, §§ 2(t), 3 (India).
[14] Digital Personal Data Protection Act, No. 22 of 2023, § 9 (India).

individual who has not completed the age of eighteen years, diverging significantly from Western frameworks like the GDPR or COPPA, which permit lower age-gates of thirteen or sixteen for digital consent.[15] Under Section 9(1), a Data Fiduciary is strictly prohibited from processing any personal data of a minor without first obtaining the "verifiable consent" of a parent or lawful guardian. Far from being toothless or completely permissive, Section 9(3) codifies absolute statutory bans, explicitly declaring that a Data Fiduciary *shall not* undertake tracking, behavioral monitoring, or targeted advertising directed at children.[16] These statutory prohibitions are backed by severe financial liabilities under the Schedule to the Act, which empowers the Data Protection Board of India (DPBI) to levy non-compliance penalties of up to ₹200 crores specifically for violations concerning the processing of children's data.[17]

Despite the statutory strength of Section 9, its practical implementation introduces profound systemic friction and analytical concerns. The structural choice to enforce a rigid, uniform age threshold of 18 completely overlooks the legal doctrine of evolving capacities, effectively stripping older adolescents of digital autonomy and restricting their access to essential educational and community spaces unless they secure parental intervention. Operationally, the mandate for "verifiable parental consent" creates an architectural paradox: to verifiably authenticate that an individual is a parent or lawful guardian, platforms must aggressively collect additional, highly sensitive telemetry such as government-issued identification tokens or financial credentials thereby directly undermining the foundational principle of data minimization and increasing the data-breach attack surface for entire households.

Additionally, with the Ministry of Electronics and Information Technology (MeitY) moving to operationalize the framework through the highly anticipated notification of the Digital Personal Data Protection Rules, the practical enforcement of these protections is set to transition heavily into the administrative domain.[18] Under Section 9(4) and Section 9(5), the Central Government retains wide-ranging delegated powers to exempt certain classes of data fiduciaries or specific processing activities if they are deemed "verifiably safe," or to lower the exempt age threshold for specific entities. This heavy reliance on executive rule-making to define operational mechanics introduces an element of regulatory

[15] Digital Personal Data Protection Act, No. 22 of 2023, § 2(f) (India); Regulation (EU) 2016/679 of the European Parliament and of the Council art. 8, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[16] Digital Personal Data Protection Act, No. 22 of 2023, § 9(3) (India).
[17] Digital Personal Data Protection Act, No. 22 of 2023, sched., item 2 (India).
[18] Ministry of Electronics & Information Technology, Digital Personal Data Protection Rules, 2025, notified Nov. 14, 2025 (India).

fluidity, making child-centric data rights highly dependent on bureaucratic implementation, corporate lobbying pressures, and administrative modifications within India's governance structure, while the newly constituted DPBI faces the monumental task of enforcing these high-stakes mandates across a vast and deeply saturated digital marketplace.

CRITICAL GAPS IN THE DPDPA'S CHILD-PROTECTIVE FRAMEWORK

The assertion that the DPDPA fails to establish explicit age-based consent thresholds or restrictions on targeted advertising contains a fundamental statutory inaccuracy that must be corrected to maintain doctoral-level legal accuracy. Section 2(f) of the Digital Personal Data Protection Act (DPDPA), 2023, establishes a definitive, blanket age-based threshold by defining a "child" as any individual who has not completed the age of eighteen years, completely bypassing any subjective baseline of nominal minor consent.[19] Far from omitting restrictions on corporate data monetization, Section 9(1) strictly mandates that a Data Fiduciary must obtain verifiable parental or lawful guardian consent before processing any personal data of a minor, while Section 9(3) codifies an absolute statutory injunction declaring that a Data Fiduciary shall not engage in tracking, behavioral monitoring, or targeted advertising directed at children.[20] These prohibitions are backed by severe financial liabilities under the Schedule to the Act, which empowers the Data Protection Board of India (DPBI) to levy penalties up to ₹200 crores specifically for violations concerning the processing of children's data, meaning platforms cannot legally justify comprehensive minor data collection for commercial optimization.[21]

However, your broader critique regarding the systemic, qualitative gaps within this framework remains highly valid and points to deep vulnerabilities within India's socio-cultural and administrative structure. By enforcing a rigid, unyielding age gate at eighteen, the DPDPA completely ignores the legal doctrine of evolving capacities recognized globally, which can inadvertently incentivize older adolescents to falsify their ages, thereby driving them deeper into unregulated digital spaces and creating a severe "consent fatigue" that burdens less digitally literate Indian parents. Furthermore, while targeted advertising is explicitly banned, the Act lacks specialized restrictions against automated, organic algorithmic profiling designed to maximize user engagement. This leaves a regulatory loophole where machine learning systems can exploit an adolescent's psychological vulnerabilities and disrupt domestic

[19] Digital Personal Data Protection Act, No. 22 of 2023, § 2(f) (India).
[20] Digital Personal Data Protection Act, No. 22 of 2023, §§ 9(1), 9(3) (India).
[21] Digital Personal Data Protection Act, No. 22 of 2023, sched., item 2 (India).

cultural values centered around education and familial balance without technically violating any codified principles. Additionally, the framework treats highly sensitive data such as data revealing an adolescent's emerging sexual orientation, gender identity, or mental health struggles identically to adult data datasets, completely overlooking localized risks like family ostracism, social marginalization, or reputational harm within the Indian socio-cultural fabric. Finally, the DPDPA applies a uniform standard for data breach notifications and international transfers without mandating expedited timelines, mandatory reporting to child protection bodies like the National Commission for Protection of Child Rights (NCPCR), or automatically classifying minor data processing as a mandatory trigger for a Data Protection Impact Assessment (DPIA), unless an entity is specifically designated as a Significant Data Fiduciary (SDF).

INDIA'S EXISTING LEGAL FRAMEWORK AND THE DPDPA'S INTEGRATION

The integration of the Digital Personal Data Protection Act (DPDPA), 2023, into India's historical child protection framework marks a critical shift toward digital safety, yet it reveals clear jurisdictional boundaries and statutory tensions. Structurally, India's child welfare architecture has long focused on reactive and punitive measures: the *Juvenile Justice (Care and Protection of Children) Act, 2015*, establishes civil obligations to protect children from physical abuse, exploitation, and neglect, while the *Protection of Children from Sexual Offences (POCSO) Act, 2012*, explicitly criminalizes digital harms such as cyber-predation and the dissemination of Child Sexual Exploitative and Abuse Material (CSEAM) under Section 15.[22] The DPDPA complements these frameworks by acting as a proactive, non-penal shield. Section 9(3) blocks the corporate profiling and behavioral tracking mechanisms that digital predators leverage to target minors, shifting the regulatory burden from downstream criminal prosecution to upstream data minimization.[23] Furthermore, the DPDPA solidifies the constitutional jurisprudence established in *Justice K.S. Puttaswamy v. Union of India (2017)*, which recognized privacy as an fundamental right under Article 21, and bridges it with socio-economic mandates like the *Right of Children to Free and Compulsory Education (RTE) Act, 2009*, by attempting to regulate the intrusive data collection practiced by commercial ed-tech platforms.[24]

Despite these complementary structures, the integration remains administratively distinct, as data protection laws generally govern

[22] Protection of Children from Sexual Offences Act, No. 32 of 2012, § 15 (India).
[23] Digital Personal Data Protection Act, No. 22 of 2023, § 9(3) (India).
[24] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

processing rather than crime detection. The DPDPA operates strictly as a data governance statute administered by the Data Protection Board of India (DPBI), and it does not explicitly create discovery mandates or intercept channels for child-protection bodies like the National Commission for Protection of Child Rights (NCPCR) or state police forces investigating POCSO violations. Law enforcement access to personal data for criminal investigations remains separately carcerally governed by procedural exemptions under the DPDPA's Section 7 frameworks, the *Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023*, and Section 69 of the *Information Technology Act, 2000*.[25] This statutory separation balances individual digital privacy with state intervention, but it leaves an administrative boundary regarding how digital fiduciaries can seamlessly share threat intelligence with law enforcement without violating their primary data fiduciary obligations to the minor.

CONCLUSION

The Digital Personal Data Protection Act (DPDPA), 2023, represents a watershed moment in India's legislative history, establishing the nation's first comprehensive statutory framework for data governance in the digital age. By codifying core principles such as purpose limitation, data minimization, and accountability, the Act provides a necessary baseline architecture for protecting personal data across India's rapidly expanding digital ecosystem. However, a critical doctrinal assessment reveals that the Act's child-protective framework remains structurally underspecified and overly reliant on delegated legislation. While Section 9 of the DPDPA introduces mandatory parental consent and statutory prohibitions against tracking and targeted advertising, the implementation of these safeguards remains tethered to executive rulemaking, creating significant regulatory fluidity. The current framework's failure to differentiate between the evolving cognitive capacities of minors treating all individuals under eighteen as a monolithic block creates friction with the global "privacy-by-design" standard, which increasingly favors tiered, age-appropriate protections. Furthermore, the Act's relative silence on the systemic harms of organic, engagement-maximizing algorithmic profiling, combined with the lack of specialized mandates for high-risk processing of children's sensitive data, leaves a profound regulatory gap regarding the psychological and sociological welfare of Indian youth.

To transition from a formalistic compliance regime to a substantive child-centric protective architecture, the Indian legislature must consider targeted amendments that move beyond generic data governance. Future reforms should prioritize the following: first, the statutory

[25] Digital Personal Data Protection Act, No. 22 of 2023, §§ 7(c)–(e) (India).

institutionalization of "Privacy by Design" and "Default Privacy" for all services accessed by minors, shifting the burden of safety from the parent to the platform's engineering architecture. Second, the framework must mandate periodic, independent algorithmic audits for Significant Data Fiduciaries (SDFs) to ensure that content-curation loops do not trigger "detrimental effects" on minor well-being a term that requires immediate, granular definition by the Data Protection Board of India (DPBI). Third, the Act should introduce expedited breach-notification protocols and mandatory reporting to child-welfare authorities, such as the National Commission for Protection of Child Rights (NCPCR), whenever children's datasets are compromised.

Ultimately, the DPDPA is a foundational instrument, but it is not a final solution. The efficacy of India's digital privacy regime will not be determined by the text of the Act alone, but by the rigor with which the DPBI enforces these mandates and the extent to which platforms are compelled to decouple their commercial business models from the exploitation of minor behavioral data. Empowering Indian parents, educators, and children through transparent, multi-lingual digital literacy initiatives is equally essential to fostering a culture of informed agency. Only through a harmonious integration of robust statutory safeguards, proactive regulatory oversight, and a commitment to prioritizing human welfare over algorithmic engagement, can India secure a digital future where its children are afforded the same dignity, safety, and autonomy online that they are guaranteed under the constitutional fabric of the nation.