INTERNATIONAL JOURNAL OF ENGINEERING MANAGEMENT AND SOCIAL SCIENCES (IJEMSS)

e-ISSN : 3139-065X

www.ijemss.com

editor@ijemss.com

Vol. 01, Issue 5, September 2026, pp :134-137

THE DIGITAL PANOPTICON: CLASSROOM SURVEILLANCE, COMMERCIAL PROFILING, AND CHILD DATA PROTECTION IN INDIA

[1]S. Swaroopa Rani

[1]Legal Professional, Educator and Social Activist; Hyderabad, Telangana, India. semasandhra@yahoo.com

DOI: https://doi.org/10.5281/zenodo.22931766

ABSTRACT

The digital transformation of the Indian educational landscape has shifted pedagogical infrastructure from localized, ephemeral spaces to cloud-based, data-extractive environments. This paper provides a comprehensive socio-legal analysis of child data protection in India, examining the structural intersection of the Digital Personal Data Protection (DPDP) Act, 2023, the fundamental right to privacy established in Justice K.S. Puttaswamy v. Union of India (2017), and emerging judicial directives. By analyzing empirical metrics regarding Educational Technology (EdTech) penetration and the parallel surge in minor-centric cybercrimes, this essay argues that Section 9 of the DPDP Act relies on an archaic model of parental protectionism. This framework strips minors of their digital agency, leaves them vulnerable to lifelong commercial profiling, and fails to account for state-sponsored surveillance in marginalized public schools. Ultimately, a rights-based, child-centric legislative overhaul is proposed to protect the evolving autonomy of India's youth.

Keywords:

Child Rights, Digital Personal Data Protection (DPDP) Act 2023, Informational Privacy, EdTech, Section 9, Puttaswamy, Algorithmic Profiling, Surveillance Capitalism, India.

1. INTRODUCTION

The contemporary Indian classroom has undergone an aggressive architectural mutation. Driven by a massive user base of over 250 million school-going children, India has positioned itself as the largest educational market by digital users globally. The domestic EdTech and smart classroom market reached a valuation of $8.87 billion, with projections to eclipse $19 billion by 2030. This expansion is not merely a shift in medium; it represents a fundamental re-engineering of pedagogical spaces. The traditional classroom—once bounded by physical geography, blackboards, and the unrecorded, ephemeral interactions between teachers and pupils—has been replaced by a continuous data-collection engine.

Every keystroke, response delay, facial expression during examinations, and algorithmic assessment interaction generates a localized data point. These data points do not exist in isolation; they are gathered, aggregated, and stored long-term by private fiduciaries and public cloud services. From automated facial recognition systems tracking daily attendance in municipal schools to AI-driven proctoring software measuring student metrics in elite institutions, a child's cognitive, behavioral, and biometric profile is systematically compiled.

While the legislature attempted to build a protective shield around minors through the Digital Personal Data Protection (DPDP) Act, 2023, the reality at the grassroots level tells a different story. The current statutory approach is fundamentally flawed. It conceptualizes the child as an object of parental custody or state administration rather than an independent rights-holder under the UN Convention on the Rights of the Child (UNCRC). As a result, the state has inadvertently authorized a digital panopticon that monitors children today and risks economically profiling them tomorrow.

2. DOCTRINAL FOUNDATIONS: FROM PUTTASWAMY TO ABHISHEK BAXI

The constitutional framework for digital child rights is anchored in the landmark Supreme Court ruling Justice K.S. Puttaswamy v. Union of India (2017). In Puttaswamy, a nine-judge bench unanimously recognized the Right to Privacy as an intrinsic part of the Right to Life and Personal Liberty under Article 21 of the Constitution of India. Crucially, the court established that informational privacy is essential to human dignity, dictating that any state or private infringement must pass a strict three-pronged test: legality, necessity, and proportionality.

When applied to the educational sector, current data-harvesting practices struggle to clear this constitutional bar. The

INTERNATIONAL JOURNAL OF ENGINEERING MANAGEMENT AND SOCIAL SCIENCES (IJEMSS)

e-ISSN : 3139-065X

www.ijemss.com

editor@ijemss.com

Vol. 01, Issue 5, September 2026, pp :134-137

state has increasingly sought to centralize student information through initiatives like the Automated Permanent Academic Account Registry (APAAR). Ostensibly voluntary, APAAR digitizes a student's entire academic journey, linking it to state databases. Recognizing the threat of coercive state tracking, the Supreme Court of India intervened directly in the landmark case Abhishek Baxi & Ors. v. Union of India & Ors. (2026). The Court issued a strict directive ordering authorities to give parents an explicit option to refuse or withhold consent for APAAR, while explicitly restricting the sharing of such data with private entities under the tenets of the DPDP Act. The Court held that data collection undertaken pursuant to an administrative scheme remains strictly subject to data protection principles.

Furthermore, the judiciary has attempted to harmonize protection with digital liberty. In Just Rights for Children Alliance v. S. Harish (2024), a division bench of the Supreme Court addressed online child safety, bridging the gap between platform intermediary liabilities and child protection by criminalizing the active possession, storage, and viewing of Child Sexual Exploitative and Abuse Material (CSEAM). This decision established a clear judicial precedent that passive consumption online directly fuels real-world exploitation cycles. Despite these strong judicial interventions, a significant disconnect remains between abstract constitutional mandates and the text of India's primary data protection law. The legislature's response—embodied in the DPDP Act—fails to scale effectively to meet these high standards of constitutional proportionality, leaving the daily practices of EdTech companies largely unchecked.

3. THE PARADOX OF SECTION 9: PARENTAL PROTECTIONISM VS. MINOR AGENCY

The primary mechanism for safeguarding children under the DPDP Act is found in Section 9, which mandates that a data fiduciary must obtain verifiable parental consent before processing any personal data belonging to a minor under 18. While designed to protect children, this provision creates three major systemic failures:

3.1. The Erasure of Evolving Capacity

The UNCRC explicitly recognizes the concept of 'evolving capacities,' acknowledging that as children mature into adolescence, their right to informational self-determination increases. By grouping a 6-year-old child and a 17-year-old adolescent under the same rigid parental consent rule, the DPDP Act cuts off older minors from accessing vital, private digital spaces. A teenager seeking confidential information on mental health support, queer identity resources, or reproductive healthcare is legally barred if their parents refuse to sign off. Recent legal field data indicates that 53.6% of minors actively lie about their age online, proving that over-regulation results in structural circumvention rather than genuine safety.

3.2. Coercive "Sign-Away" Culture

In Indian schools, parents face an immense power imbalance. During admission, they are handed dense, multi-page terms-of-service documents by schools acting as conduits for third-party EdTech corporations. Parents lack the digital literacy to audit these platforms, and refusing to sign means their child faces exclusion from mandatory online assignments and digital classrooms. Consent in this environment is not free or informed; it is structurally coerced.

3.3. The "Detrimental Effect" Definition Vacuum

Section 9 prohibits data processing that is likely to cause 'any detrimental effect on the well-being of a child'. However, the statute leaves 'detrimental effect' entirely undefined. It remains unclear whether algorithmic behavioral profiling, targeted behavioral advertisements, or the continuous tracking of a student's cognitive dropouts constitute a legally recognized harm.

4. EMPIRICAL REALITIES: THE SURGE IN EDTECH EXPLOITATION AND CYBERCRIME

The push for digitization has run far ahead of child-centric cybersecurity infrastructure. National Crime Records Bureau (NCRB) data reveals an alarming trend: while overall crime rates in India fell by approximately 6%, cybercrime cases jumped by nearly 17.9%, crossing the one-lakh mark annually.

Table 1

Statistical Trends in Minor-Centric Cybercrimes and Exploitation

Metric Profile	Statistical Trend / Data Value
Total Crimes Against Children	Increased by 5.9% (1,87,702 cases)
Minor Cybercrime Profile	9 out of 10 involve explicit CSEAM

INTERNATIONAL JOURNAL OF ENGINEERING MANAGEMENT AND SOCIAL SCIENCES (IJEMSS)

e-ISSN : 3139-065X

www.ijemss.com

editor@ijemss.com

Vol. 01, Issue 5, September 2026, pp :134-137

FIR Conversion Discrepancy	Only 2.4% of total NCRP complaints

Note. Data compiled from the National Crime Records Bureau (NCRB) annual report metrics. CSEAM = Child Sexual Exploitative and Abuse Material; NCRP = National Cyber Crime Reporting Portal; FIR = First Information Report.

This environment of low enforcement and rising crime is particularly dangerous when coupled with EdTech data aggregation. Platforms routinely track typing patterns, webcam micro-expressions during assessments, and localized IP data to feed adaptive learning algorithms. This information is stored long-term, forming a permanent digital resume. A child labeled as 'low-attentive' or 'under-performing' by an algorithm at age nine could face predictive discrimination a decade later when applying for university admissions, student loans, or employment. This long-term commercial profiling represents a severe violation of the right to an uncommodified childhood.

5. THE INTERSECTIONAL FAULTLINE: CORPORATE PROFILING VS. STATE SURVEILLANCE

The digital child rights crisis in India is stratified by socio-economic class. The type of privacy invasion a child faces depends heavily on the school they attend:

- **The Urban/Elite Tier (Corporate Profiling):** In high-fee private academies, children are exposed to intense commercial exploitation. Their educational metrics are processed by private data fiduciaries to build behavioral consumer profiles, optimizing them for targeted advertisements and future monetization.
- **The Public/Marginalized Tier (State Surveillance):** In low-income government schools, the primary threat is not corporate marketing, but unmonitored state surveillance. Under the banner of state modernization, local administrations have deployed biometric devices and automated facial recognition cameras in classrooms. This data is often linked directly to state identity databases like Aadhaar. For underprivileged youth, the classroom has been converted into an experimental ground for state surveillance without their explicit knowledge or consent, normalizing monitoring from an early age.

6. POLICY RECOMMENDATIONS: A RIGHTS-BASED REMEDIAL PATH

To realign India's digital educational infrastructure with the constitutional protections of Puttaswamy and global human rights standards, the state must transition from a model of absolute parental protectionism to one of child empowerment:

- **Codify Tiered, Evolving Consent:** The DPDP Act should be amended to introduce a tiered age of consent. Adolescents aged 14 to 18 should have the autonomy to consent to the processing of their personal data for educational, health, and non-commercial services, preventing parental gatekeeping from blocking essential digital access.
- **Mandate Child Rights Impact Assessments (CRIAs):** No EdTech platform should be deployed in a public or private classroom without undergoing an independent, prior CRIA. These assessments must audit data minimization policies and ensure algorithms do not exploit minor cognitive vulnerabilities.
- **Enforce Strict Purpose Limitation and Data Firewalls:** The law must state that any personal information collected for educational evaluation cannot be shared, sold, or repurposed for commercial profiling or predictive behavioral analysis. Data must be automatically deleted once a student completes a course or graduates.
- **Establish Algorithmic Auditing for Educational Institutions:** A centralized body under the Data Protection Board (DPB) should explicitly define 'detrimental effects' to include hyper-targeted tracking, behavioral modification algorithms, and persistent consumer profiling of students.

7. CONCLUSION

The aggressive transformation of Indian classrooms from physical, localized spaces into data-extractive environments demands an urgent recalibration of the nation's legal landscape. As this paper has demonstrated, the current framework of the Digital Personal Data Protection (DPDP) Act, 2023, is fundamentally ill-equipped to shield minors from the compounding threats of corporate profiling and state-sponsored surveillance. By relying on an outdated model of absolute parental protectionism under Section 9, the legislature has effectively erased the evolving digital agency of adolescents, while failing to check the coercive 'sign-away' consent culture permeating educational institutions. Consequently, marginalized public school students are subjected to normalized state monitoring, while elite students face aggressive commercial commodification.

INTERNATIONAL JOURNAL OF ENGINEERING MANAGEMENT AND SOCIAL SCIENCES (IJEMSS)

e-ISSN : 3139-065X

www.ijemss.com

editor@ijemss.com

Vol. 01, Issue 5, September 2026, pp :134-137

This statutory failure stands in direct contradiction to the constitutional thresholds of necessity, legality, and proportionality established by the Supreme Court in Justice K.S. Puttaswamy v. Union of India. While recent judicial interventions—such as the restriction of centralized tracking in Abhishek Baxi (2026) and the enforcement of platform liabilities in Just Rights for Children Alliance (2024)—indicate a growing judicial consciousness of digital harms, piecemeal litigation cannot substitute for structural legislative reform.

To dismantle this digital panopticon, India must transition toward a rights-based, child-centric legislative framework. This requires codifying tiered age consent models, mandating strict prior Child Rights Impact Assessments (CRIAs) for EdTech deployment, and enforcing absolute data firewalls to prevent permanent behavioral profiling. Protecting the evolving autonomy of India's youth requires ensuring that digital education does not demand the surrender of fundamental privacy. The classroom must remain a sanctuary for intellectual exploration and cognitive development, rather than serving as a monetization pipeline or an experimental ground for tracking future citizens.

REFERENCES

1. Abhishek Baxi & Ors. v. Union of India & Ors., W.P. (C) No. 456/2025 (Supreme Court of India 2026).
2. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
3. Just Rights for Children Alliance v. S. Harish, C.A. No. 8912/2023 (Supreme Court of India 2024).
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
5. National Crime Records Bureau. (2025). Crime in India 2024: Statistics volume II. Ministry of Home Affairs, Government of India.
6. UN General Assembly. (1989). Convention on the Rights of the Child. United Nations, Treaty Series, vol. 1577, p. 3.
7. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

DISCLAIMER

The views and opinions expressed in this work are solely those of the author(s) and do not necessarily reflect the official policy or position of any educational institution, government body, or regulatory authority. The analysis provided is based on publicly available academic literature and legal frameworks, including India's **Digital Personal Data Protection (DPDP) Act**, and is intended strictly for educational and scholarly purposes. The information, analysis, and commentary contained in this document are for **general informational and educational purposes only**. They do not constitute formal legal advice, nor do they establish an attorney-client relationship.