The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CHILDREN'S DATA PROTECTION IN INDIA: STRIKING THE RIGHT LEGAL BALANCE BETWEEN SAFETY AND INNOVATION

Sukhvinder Singh

ABSTRACT

This piece critically analyzes the shifting legal framework of children's protection of data in India, balancing the protection of child privacy with the promotion of digital innovation. It tours constitutional guarantees recognizing the right to privacy and child well-being, statute law like the Digital Personal Data Protection Act, 2023, and milestone judgments defining protections for children's personal data in the digital space. The research sets out structural and operational concerns, such as overly broad age limits, practical issues with parental consent, and dangers of strangling innovation with disproportionate regulation. Taking comparative learning from international models such as the GDPR, COPPA, and the UK's Age-Appropriate Design Code, the article suggests a proportionate approach based on the best interests of the child principle.This requires a systematic legal framework, cooperative industry practices, privacy-by-design considerations, and effective judicial oversight. In the end, the article calls for balanced reforms that promote children's digital dignity and safety and enable India's ongoing technological growth and socio-economic development.

Keywords: Privacy, Children, Data Protection, Consent, Innovation, Regulation, Safeguards

INTRODUCTION

The digital age has significantly changed the landscape of privacy, especially for children, whose presence in cyberspace is getting stronger but weaker. Privacy, which is now an essential right in India, is being faced with unprecedented challenges in a society characterised by rapid technological advances, widespread digitalisation, and low digital literacy among children. Children, as they gain from exposure to information and digital resources for learning and

creativity, at the same time confront risks—surveillance, manipulation, profiling, and exploitation. The legal response of India to all these is changing and is seeking to safeguard child users without dampening digital innovation essential for socio-economic growth. This article undertakes a legal examination of the constitutional, statutory, and judicial boundaries of children's data protection in India, referencing comparative lessons from international frameworks, highlighting inherent challenges, and speculating on potential directions for balancing security with innovation.

While there is a burgeoning regulatory landscape, India's approach to children's data protection is in the balance—torn between the needs of child safety and the need to create a healthy digital economy. The current legal landscape, its patchwork of judicial dicta, legislation, and constitutional provisions, remains unfinished in operationalisation, effectiveness, and adaptability. The task is to design a system that effectively realizes privacy as a right for the child, with robust safeguards and accountability, but not stifling innovation and entrepreneurship essential for digital India.

CONSTITUTIONAL FRAMEWORK

Article 21 of The Indian Constitution:- The Right to Privacy

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court unequivocally held privacy to be a fundamental right and extended it specifically to informational privacy in information technology times. For children, this right has to be protected against arbitrary or disproportionate collection, storage and access to their own personal data considering their particular vulnerabilities.[1]

Article 39(f) of The Indian Constitution:- Directive Principle of Child Welfare

It instructs the State to guarantee that children are afforded opportunities and resources to develop healthily and in environments of freedom and respect. Although not enforceable per se, this directive principle overwhelmingly justifies provisions on data governance related to children's all-round growth, digital dignity and progress in safe virtual environments.[2]

Article 15(3) of The Indian Constitution :- Protective Discrimination

It allows the State to extend special treatment to children. This constitutional justifies differentiated data protection regimes or further child protections beyond the regime for adults, which can be

[1] Constitution of India, Art 21
[2] Constitution of India, Art 39(f).

justified through legislative steps such as parental consent, enhanced notice requirements and child sensitised disclosure rules.[3]

Article 19(1)(g) of Indian Constitution :- Innovation and Reasonable Restrictions

It guarantees freedom to exercise any profession or occupation, including freedom to innovate technologically in cyber spaces. Limitations imposed for child protection or privacy—such as data localisation, age-gating, or required design standards—must also undergo the test of reasonableness in Article 19(6). Hence, India's constitutional scheme requires a nuanced balancing between innovators' rights and the requirement of child data protection. In TMA Pai Foundation v. State of Karnataka, the Court grappled with the ways in which control mechanisms must balance constitutional rights and safeguards that are necessary, a principle that has its roots in innovation in child-centered digital environments.[4]

STATUTORY LANDSCAPE OF CHILDREN'S DATA PROTECTION IN INDIA

Digital Personal Data Protection Act, 2023

This act is a turning point in the data governance in India, making consent the foundation of processing personal data and imposing strict obligations pertaining to children. The Act defines 'child' as any individual below the age of eighteen, requires parental consent that is verifiable in the process of handling children's data, and bans tracking, targeted advertizing, or any "processing likely to cause detriment." Yet, the Act's scope-refusing to differentiate between older teenagers and younger kids- and lack of precise implementation guidelines have questioned its practicality and proportionality.[5] In Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal, the Supreme Court made it clear State regulation of digital broadcasting should not unfairly limit innovation, while child protection regulations are warranted. The case provides guidance in interpreting proportionality when complying with IT and DPDP Act for child-users.[6]

Information Technology Act, 2000 And IT Rules 2021

Though the act is non-child specific, but it criminalizes the online content that is detrimental to children and prescribes penalties for contraventions.[7] The Information Technology Rules, 2021

[3] Constitution of India, Art 15(3).
[4] *TMA Pai Foundation* v *State of Karnataka* (2002) 8 SCC 481.
[5] Digital Personal Data Protection Act, 2023, s 9, 10.
[6] *Secretary, Ministry of Information & Broadcasting* v *Cricket Association of Bengal* (1995) 2 SCC 161.
[7] Information Technology Act, 2000, s 67B.

mandate due diligence responsibilities (notification, takedown mechanisms and age-gating) on platforms which are available to children. However, enforcement is haphazard and redress mechanisms convoluted, especially for child complainants.[8]

The Protection of Children from Sexual Offences Act (POCSO), 2015

The POCSO act is a offline as well as online child sexual offence criminal law which mandates intermediaries to report child pornography and connected offences, being a coming together of criminal law as well as data protection and not really solving the large data privacy issues.[9]

Juvenile Justice (Care And Protection Of Children) Act, 2015

The JJ Act makes the recording and information about children in conflict with the law or in need of care and protection confidential, placing statutory duties on several authorities. Though not a uniform data protection legislation, it makes certain the principles of data minimisation, access restricted, and confidentiality in certain circumstances.[10]

JUDICIAL DEVELOPMENTS

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017):- The Supreme Court's overall privacy decision set the tone for later data protection frameworks. The Court emphasized the "best interests of the child" principle, citing the UNCRC and international standards. Even though the ruling did not rule on children's data in particular, its understanding of privacy as personal autonomy and dignity ineluctably extends to minors, who need special protection by reason of the limited capacity of children to understand risks and to assent informed.[11]

Sabu Mathew George v. Union of India (2015):- In this case, the Supreme Court instructed online sites and search engines to actively block sex selection content, making intermediaries responsible for child-protective compliance with the Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act. The case highlights the judiciary's receptivity to instructing technology firms on child protection at the expense of tension with innovation and speech interests.[12]

---

[8] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 3, 4.
[9] Protection of Children from Sexual Offences Act, 2012.
[10] Juvenile Justice (Care and Protection of Children) Act, 2015, s 74.
[11] *Justice K.S. Puttaswamy (Retd.)* v *Union of India* (2017) 10 SCC 1.
[12] *Sabu Mathew George* v *Union of India* (2015) 11 SCC 545.

Prajwala Letter Case (2015) :- Seizing suo motu cognizance on the basis of a letter that revealed the online dissemination of child sexual abuse content, the Supreme Court laid down directions that mandated online platforms to actively block and report unlawful content. The case reasserted the role of intermediaries as data fiduciaries and reflected judicial intent to implement strict child protection standards in the virtual world. It promoted the privacy, dignity, and security of children in cyberspace through active judicial monitoring.[13]

Sheela Barse v. Union of India: Confirmed expansive State responsibility for children's welfare and privacy, tracking custodial and institutional care standards that similarly can inform privacy-by-design requirements for children's online spaces.[14]

Bachpan Bachao Andolan v. Union of India: Applied the best interests principle to policy, with the Court ordering rigorous protections for children in trafficking and exploitation situations—the justification now widely embraced for children's online safety too.[15]

Avinash Mehrotra v. Union of India: Established the "best interests of the child" test for regulatory frameworks (in that instance, school fire safety) but acknowledged the need for supervision and code adherence—pertinent to co-regulatory digital safety frameworks.[16]

Supreme Court Legal Services Committee v. Union of India: Upheld anonymity and dignity of child victims by allowing in-camera proceedings and limiting reporting, a principle vital for confidentiality of children's information.[17]

COMPARATIVE PERSPECTIVE

European Union: GDPR Article 8

The General Data Protection Regulation (GDPR) established a worldwide model for protecting children's data, notably through Article 8, which imposes a minimum age of 16 (or a lower one, not below 13, in certain cases) for online service consent, unless parental authorisation is not required.

[13]Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations (08.01.2018 - SC) : MANU/SC/0193/2018

[14] *Sheela Barse* v *Union of India* (1986) 3 SCC 596.

[15] *Bachpan Bachao Andolan* v *Union of India* (2011) 5 SCC 1.

[16] *Avinash Mehrotra* v *Union of India* (2009) 6 SCC 398.

[17] *Supreme Court Legal Services Committee v Union of India* (2012) 6 SCC 771.

The GDPR also imposes child-friendly privacy notices and 'privacy by design' on platforms aimed at children.[18]

United States: COPPA

The Children's Online Privacy Protection Act (COPPA) regulates online data collection from children younger than 13 years, requiring parental permission, notice, and the ability to review or delete the child's information. COPPA's comparatively low age limit and emphasis on operation of parental consent have influenced corresponding provisions in Indian law but have been criticized for being impracticable at scale.[19]

United Kingdom: Age-Appropriate Design Code

The UK's Age-Appropriate Design Code is more than consent, requiring privacy by default, age-appropriate information, and minimizing nudge methods for every user under the age of 18. It also promotes risk assessments, openness, and assertive child-centricity in digital design—avoiding exploitation and profiling.[20]

LEGAL CHALLENGES

Overbroad Age Threshold: Indian law is uniform in treating all minors below 18 equally, inconsistent with worldwide practice that distinguishes between age and levels of maturity. This will result in over-protecting mature adolescents, thus infringing upon their digital autonomy, and holding platforms accountable for unrealistic consent processes.

Practicability of Parental Consent: It is technologically and infrastructurally difficult to collect verifiable parental consent at scale, particularly in a low-digital-literacy country with shared devices and false age declarations. This either risks excluding children from digital services or incentivizes non-compliance.

Proportionality and Chilling Innovation: Blanket bans on processing, monitoring, or advertising to children—albeit with good intent—could potentially fall short of the proportionality requirement under Article 21 and lead to disproportionate compliance costs, stifling educational apps or health tech development.[21]

---

[18] General Data Protection Regulation, Regulation (EU) 2016/679, Art 8.
[19] Children's Online Privacy Protection Act, 15 USC §§ 6501–6506 (United States, 1998).
[20] Information Commissioner's Office (UK), Age-Appropriate Design Code (2020).
[21] Nandan Kamath, 'The Challenge of Protecting Children Online in India' (2020) 8 NLUD Journal of Legal Studies 1, 24-25.

Fragmented Enforcement and Accountability: Several overlapping statutes create jurisdictional complexities, watered-down accountability, and fragmented enforcement. Regulator bodies like the Data Protection Board and current agencies could be short on child-specialist knowledge or coordination capacities.

Innovation Limitations: Strict design and compliance requirements can discourage start-ups and developers from developing child-focused products or expanding digital learning, particularly where compliance is expensive. Compliance is likely to become an innovation obstacle.

BALANCING SAFETY AND INNOVATION

Graded or Age-Banded Framework: Laws can take a differential approach—differentiating between children (0-12), adolescents (13-17), and "mature minors"—thus basing protection on capacity and context. This would be in line with international practice and provide limited autonomy with protection in adolescent groups.

Best Interests of the Child (UNCRC): Adopting the UNCRC best interests of the child principle as an interpretative guiding benchmark guarantees that children's changing capacities and best standards of welfare, as opposed to protection alone, continue to be the focus of law and policy. Indian courts have already established this integrated principle in several judgments.[22]

Co-Regulation and Industry Standards: In place of command-control systems, India can encourage platforms to comply with co-regulatory codes—like privacy certification, self-regulatory audits, and implementation of the 'Age-Appropriate Design Code' model.

Effective Judicial Oversight: The courts need to remain vigilant as checks—issuing guidelines for privacy-intrusive technologies, guaranteeing proportionate restrictions, and deciding on the reasonableness of legislative or executive action.

Privacy by Design: Statute and compliance requirements need to promote privacy-by-design for ed-tech, social media, and entertainment apps for children—prioritizing data minimisation, contextual integrity, and stringent breach notification procedures. Tech-based solutions (age estimation, digital literacy components, and real-time detection of risks) should be promoted.

CONCLUSION

[22] United Nations Convention on the Rights of the Child (1989), Art 3(1).

India's protection regime for children's data is at the juncture of two important commitments: ensuring the dignity and privacy of its youngest citizens and creating a globally competitive digital environment. The constitutional and legislative architecture, while strong in intent, must evolve—towards sophisticated, context-responsive, and enforceable provisions based on children's actual best interests. Reforms through legislation must avoid excessive paternalism as well as minimum-state laissez-faire approaches, striving towards a dynamic balance. Judicial supervision, legislative creativity, and regulatory clarity on the basis of international best practices and India's socio-cultural landscape are the keys to making the digital environment safer, fairer, and more enriching for Indian children.