
DIGITAL PRIVACY PROTECTION FOR YOUNG USERS IN THE DIGITAL ERA: REGULATORY CHALLENGES, CONSTITUTIONAL SAFEGUARDS, AND LEGISLATIVE REFORMS IN INDIA

***Manisha Kumari**

Department of Law Haveli Institute of Legal Studies and Research University of Mumbai.

Article Received: 13 August 2026

***Corresponding Author: Manisha Kumari**

Article Revised: 03 September 2026

Department of Law Haveli Institute of Legal Studies and Research University of Mumbai.

Published on: 23 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.7249>

ABSTRACT

The rapid proliferation of digital technologies, mobile applications, online gaming platforms, and smart devices has fundamentally altered how children and adolescents interact with the digital ecosystem. While the internet offers unprecedented opportunities for education, social interaction, and cognitive development, it simultaneously exposes young users to unprecedented privacy risks, intrusive data surveillance, behavioral profiling, and dark patterns designed to exploit psychological vulnerabilities. Children, owing to their evolving mental capacities, are often incapable of granting informed, meaningful consent, making them exceptionally vulnerable in a data-driven economy where personal information is aggressively monetized.

This comprehensive research dissertation critically examines the legal, constitutional, and regulatory frameworks governing the digital privacy protection of young users in India. It analyses the constitutional guarantees under Article 21 (Right to Privacy), Article 14 (Equality and Protection against Arbitrary Exploitation), and Article 39(f) of the Directive Principles of State Policy. Furthermore, this study evaluates the efficacy of India's statutory framework, primarily focusing on the Digital Personal Data Protection Act (DPDP Act), 2023, the Information Technology Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012.

By contrasting Indian legislation with international gold standards—specifically the United States' Children's Online Privacy Protection Act (COPPA) and the European Union's General Data Protection Regulation (GDPR)—this paper identifies critical regulatory lacunae, including age-verification hurdles, consent fatigue, parental tracking paradoxes, and dark

pattern manipulations in mobile gaming environments. The paper concludes with actionable legislative, technological, and judicial recommendations to establish a robust, child-centric, and human-rights-focused digital governance model in India.

KEYWORDS: Digital Privacy, Young Users, Child Data Protection, DPDP Act 2023, Article 21, Dark Patterns, Behavioral Profiling, COPPA, GDPR, Cyber Safety, Algorithmic Surveillance, Age Verification.

1. INTRODUCTION AND BACKGROUND OF THE STUDY

The twenty-first century has witnessed an exponential surge in digital connectivity, transforming the internet from a luxury information retrieval mechanism into an essential infrastructural utility for education, communication, entertainment, and personal identity formation. In India—a nation undergoing a massive digital metamorphosis driven by affordable smartphones and ubiquitous high-speed mobile broadband—children and young users constitute one of the fastest-growing demographics in the online space. According to recent national usage metrics, millions of minors regularly access mobile gaming applications, social media networks, e-learning platforms, and digital streaming services.

However, this rapid digital integration has unfolded within an online ecosystem primarily engineered for commercial data harvesting. Young users navigate digital environments that actively collect, analyze, and trade personal identifiers, location metrics, browsing histories, search queries, contact lists, and behavioral traits. Unlike adults, children and young adolescents lack the cognitive maturity, risk awareness, and legal literacy necessary to comprehend the long-term consequences of extensive digital footprints. Consequently, they become primary targets for continuous algorithmic surveillance, predatory targeted advertising, and covert psychological manipulation.

The issue of digital privacy protection for young users is not merely a technical or regulatory concern; it is fundamentally a human rights and constitutional imperative. Unrestricted data collection and algorithmic profiling directly impinge upon a minor's dignity, autonomy, personal safety, and freedom of thought. In the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*, the Supreme Court of India solemnly affirmed that the Right to Privacy is an intrinsic component of the Right to Life and Personal Liberty guaranteed under Article 21 of the Constitution. Extending this constitutional protection to children requires specialized legal mechanisms that balance the minor's right to digital participation with their fundamental right to be protected from commercial exploitation and

digital harm.

This extensive dissertation provides an exhaustive analytical inquiry into the legal regime governing young users' digital privacy in India. It examines statutory mechanisms, assesses judicial precedents, scrutinizes international legal frameworks, highlights systemic challenges in the age of generative AI and online gaming, and offers concrete legislative remedies.

2. STATEMENT OF THE PROBLEM AND RESEARCH METHODOLOGY

2.1 Statement of the Problem

Modern internet architecture relies on data monetization models that incentivize maximum data extraction. Children, due to their developmental stage, do not possess the capacity to understand privacy policies written in complex legal jargon, nor do they understand how their personal data is aggregated, profiled, and resold. While legislative frameworks such as the Digital Personal Data Protection Act (DPDP Act), 2023 attempt to safeguard children through mandatory parental consent, this approach introduces technical, practical, and constitutional friction. Issues such as over-collection of parental data for verification, "consent fatigue," age evasion, dark patterns, and intrusive in-game monetization strategies remain inadequately addressed. Therefore, a critical legal evaluation is required to bridge the gap between abstract privacy guarantees and actionable child online safety.

2.2 Objectives of the Research

- To evaluate the constitutional foundation of child privacy rights under Part III and Part IV of the Constitution of India.
- To analyze the statutory protection mechanism provided under Section 9 of the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000.
- To identify key digital threats facing young users, including algorithmic profiling, manipulative dark patterns, location surveillance, and predatory in-game mechanics.
- To conduct a comparative analysis of Indian child data protection laws with global legal frameworks, particularly COPPA (USA) and GDPR (European Union).
- To propose concrete legislative, technological, and administrative reforms for building a child-centric privacy ecosystem in India.

2.3 Research Methodology

This study adopts a **doctrinal, analytical, and comparative legal methodology**. The inquiry relies on authoritative primary legal sources, including the Constitution of India,

parliamentary statutes, rules, and judicial precedents from the Supreme Court and various High Courts. Additionally, international instruments such as the United Nations Convention on the Rights of the Child (UNCRC) and comparative foreign legislations are thoroughly analyzed. Secondary sources including academic journal articles, reports by NITI Aayog, MeitY, UNICEF, and policy white papers are incorporated to contextualize the legal analysis.

3. CONSTITUTIONAL LANDSCAPE OF PRIVACY FOR MINORS IN INDIA

The constitutional architecture of India serves as the benchmark against which all legislative actions and commercial practices are measured. Although the term "privacy" is not explicitly mentioned in the text of the Constitution of India, judicial activism and expansive interpretation have established privacy as an inviolable fundamental right.

3.1 Article 21: Informational Privacy, Autonomy, and Human Dignity

In the path-breaking decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*, a nine-judge bench of the Supreme Court recognized that privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21. The Court categorized privacy into three dimensions: spatial privacy, decision-making privacy, and informational privacy.

Informational privacy is particularly crucial for young users. It recognizes that an individual should have control over their personal data and the ability to determine what information is communicated to the public. For young individuals in their formative years, excessive data monitoring by commercial entities restricts their psychological freedom, limits their ability to explore digital spaces without judgment, and creates permanent digital records that can unfairly influence their adult lives.

3.2 Article 14: Non-Arbitrariness and Cognitive Power Imbalance

Article 14 guarantees equality before the law and protection against arbitrary state and non-state action. In the digital marketplace, an extreme cognitive power asymmetry exists between multinational technology conglomerates and young users. Tech companies utilize sophisticated behavioral psychology and machine learning to manipulate user interface design, forcing young users into consenting to intrusive data practices. Applying Article 14 principles ensures that platforms cannot impose unconscionable, arbitrary, or predatory terms of service on vulnerable young users.

3.3 Article 39(f): Directive Principles of State Policy

Article 39(f) places a constitutional obligation on the State to ensure that children are given opportunities and facilities to develop in a healthy manner and in conditions of freedom and dignity, and that childhood and youth are protected against exploitation and moral/material

abandonment. In the context of the 21st century, "exploitation" extends beyond physical labor to include digital exploitation, data harvesting, and psychological manipulation in online spaces.

4. STATUTORY FRAMEWORK GOVERNING DIGITAL DATA OF CHILDREN IN INDIA

4.1 The Digital Personal Data Protection (DPDP) Act, 2023: Section 9 Analysis

The DPDP Act, 2023 represents India's primary legislation dedicated to personal data governance. Section 9 of the Act specifically lays down mandates regarding the processing of children's personal data. Under Section 2(f), a "child" is defined as an individual who has not completed eighteen years of age.

Provision	Statutory Mandate (DPDP Act, 2023)	Practical & Legal Challenges
Section 9(1)	Mandates obtaining verifiable parental consent before processing any personal data of a child or a person with disability.	Implementation hurdles regarding age verification methods; risk of collecting sensitive identification documents from parents.
Section 9(2)	Prohibits Data Fiduciaries from undertaking processing of personal data that is likely to cause any detrimental effect on the well-being of a child.	Lack of statutory definition or clear guidelines on what constitutes a "detrimental effect" on child well-being.
Section 9(3)	Strictly prohibits behavioral monitoring, tracking, or targeted advertising directed toward children.	Circumvention by digital platforms through contextual ads or failure to classify content appropriately for minors.
Section 9(4)	Empowers the Central Government to exempt certain Data Fiduciaries or lower the age threshold for specific safe processing activities.	Potential regulatory dilution if broad exemptions are granted to major tech monopolies under government notifications.

4.2 The Information Technology Act, 2000 and Intermediary Rules, 2021

The Information Technology (IT) Act, 2000, along with the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, provides administrative and penal frameworks to regulate digital intermediaries and safeguard online safety:

- **Section 66E (Violation of Privacy):** Penalizes intentional capturing, publishing, or

transmitting images of private areas of an individual without consent.

- **Section 67B (Child Sexual Exploitation Material):** Imposes strict criminal liability with imprisonment for browsing, downloading, creating, publishing, or transmitting material depicting children in sexually explicit or abusive situations online.
- **Intermediary Due Diligence:** Mandates social media platforms to remove harmful, illegal, or abusive content targeted at minors within specified statutory timelines upon receiving valid notices.

4.3 Protection of Children from Sexual Offences (POCSO) Act, 2012

While POCSO is primarily a penal law designed to protect children from sexual offenses, its provisions extend to the digital domain under Sections 13, 14, and 15 regarding cyber-grooming, digital harassment, and the collection or dissemination of child pornography. The strict penal liability under POCSO intersects with digital privacy, obligating platforms to maintain rigorous safety mechanisms.

5. KEY PRIVACY THREATS AND VULNERABILITIES IN MODERN DIGITAL PLATFORMS

5.1 Algorithmic Profiling and Continuous Surveillance

Modern mobile applications and social platforms rely on complex recommendation algorithms designed to maximize user engagement. These systems track infinite data points—including keystroke dynamics, screen hover duration, content preferences, and active hours. For young users, continuous profiling creates filter bubbles that exacerbate psychological distress, encourage body dysmorphia, and reinforce compulsive screen usage.

5.2 Deceptive User Interface Practices: Dark Patterns

Dark patterns are deliberate design choices engineered into digital interfaces that manipulate users into taking actions contrary to their intent or best interests. In platforms frequented by young users, common dark patterns include:

- **Forced Continuity & Hidden Subscriptions:** Automatically transitioning free trials into paid subscriptions without clear notification to parents.
- **Disguised Advertisements:** Presenting commercial advertisements as playable game levels or essential educational resources.
- **Privacy-Intrusive Defaults:** Setting account profiles, location sharing, and direct messaging visibility to "Public" by default during account registration.

- **Nagging & Social Pressure:** Repeatedly prompting young users to connect their personal address books or social media accounts to gain virtual rewards.

5.3 The Age Verification and Parental Consent Paradox

Section 9(1) of the DPDP Act mandates "verifiable parental consent." However, executing this requirement creates significant operational and privacy dilemmas:

1. **Over-Collection Paradox:** To verify parental identity, platforms often demand official identity documents (such as Aadhaar, Passport, or PAN) or credit card verifications. This creates massive centralized data repositories containing highly sensitive adult identifiers, elevating cybersecurity risks.
2. **Consent Fatigue:** Parents flooded with constant permission requests across numerous apps routinely grant blanket permissions without reading lengthy privacy policies, rendering legal consent ineffective.
3. **Circumvention & Fake Accounts:** Minors regularly bypass age verification barriers by entering false birth dates or using adult credentials, defeating the statutory objective.

5.4 Intrusive Data Practices in Mobile Gaming & Ed-Tech Platforms

Mobile gaming applications represent a major area of concern regarding minor privacy. Many free-to-play mobile games harvest excessive device permissions—including microphone access, contact lists, exact GPS locations, and persistent device IDs—that bear no relation to game mechanics. Furthermore, mechanics such as "loot boxes" and pay-to-win micro-transactions exploit cognitive vulnerabilities, encouraging minors to share financial data or engage in unauthorized spending.

6. COMPARATIVE ANALYSIS: GLOBAL LEGAL FRAMEWORKS

India's legislative efforts can be evaluated by comparing them with established international legal frameworks that have regulated child privacy for years.

6.1 United States: Children's Online Privacy Protection Act (COPPA)

Enacted in 1998 and regulated by the Federal Trade Commission (FTC), COPPA applies to commercial websites and online services directed at children under 13 years of age.

- **Strengths:** Requires explicit, prominent privacy policies; mandates prior verifiable parental consent before data collection; grants parents the absolute right to review, delete, or refuse further data collection of their child's data.
- **Weaknesses:** COPPA's protections terminate at age 13, leaving adolescents aged 13 to

17 entirely exposed to commercial data exploitation and behavioral profiling.

6.2 European Union: General Data Protection Regulation (GDPR) & Age-Appropriate Design Code

The European Union offers a comprehensive and flexible approach to child data governance through Article 8 of the GDPR and specialized national codes:

- **Flexibility in Age Threshold:** GDPR sets the default age of digital consent at 16, but allows member states to lower it up to 13 years (e.g., UK set it at 13, Germany at 16).
- **Right to Erasure ("Right to Be Forgotten"):** Article 17 of GDPR provides young users a robust right to obtain erasure of their personal data without undue delay, ensuring that mistakes made during childhood do not permanently haunt individuals in adulthood.
- **Age-Appropriate Design Code (AADC / Children's Code):** Pioneer in the UK, the AADC sets 15 standards that digital services must follow. It mandates high privacy settings by default, turns off location tracking by default, prohibits dark patterns, and enforces rigorous "best interests of the child" risk assessments.

7. MAJOR FINDINGS AND CRITICAL LEGAL VACUUMS IN INDIA

Following a detailed analysis of Indian statutes, judicial decisions, and global legal standards, the following critical gaps in India's regulatory framework are identified:

1. **Rigid Age Categorization:** Defining every individual under 18 years as a "child" without distinction creates practical hurdles. A 7-year-old child and a 17-year-old teenager have vastly different cognitive abilities and educational needs. Treating them identically under Section 9 restricts older teenagers from exercising autonomy and accessing educational digital resources.
2. **Absence of Statutory Privacy-by-Design Obligations:** Unlike the UK's Age-Appropriate Design Code, Indian law lacks explicit statutory design requirements that obligate app developers to build privacy protections into their technical infrastructure by default.
3. **Inadequate Enforcement Mechanisms for Dark Patterns:** Although the Central Consumer Protection Authority (CCPA) issued dark pattern guidelines in late 2023, specialized technical audit mechanisms and penalties tailored to minor privacy in mobile gaming remain underdeveloped.
4. **Risk of Over-Surveillance by Parents:** Mandatory parental consent frameworks can inadvertently facilitate continuous parental tracking of adolescents, infringing upon their

evolving capacity for decision-making privacy and digital self-determination.

8. RECOMMENDATIONS AND POLICY SUGGESTIONS

To establish a balanced, future-ready, and child-centric digital privacy architecture in India, the following legislative, administrative, and technical measures are recommended:

8.1 Legislative Reforms

- **Adopt a Tiered Age System:** Amend Section 9 of the DPDP Act to introduce a two-tier age model:
 - *Under 13 Years:* Mandatory verifiable parental consent required for all personal data processing.
 - *Ages 13 to 18 Years:* Autonomous digital consent allowed for standard educational and social services, combined with an absolute statutory ban on behavioral profiling, targeted ads, and dark patterns.
- **Enact an Indian Age-Appropriate Design Code (AADC):** MeitY should frame formal statutory guidelines obligating platforms to maintain maximum privacy settings by default, disable background geolocation tracking, and eliminate infinite-scroll mechanics for minors.
- **Incorporate the Right to Erasure for Youth:** Expressly guarantee an absolute, hassle-free right to data erasure for all content posted by individuals before turning 18.

8.2 Technical and Administrative Reforms

- **Implement Zero-Knowledge Proof (ZKP) Age Verification:** Promote privacy-preserving technology like Zero-Knowledge Proofs, allowing platforms to confirm a user's age category without harvesting personal identification documents or biometric data.
- **Establish a Child Digital Safety Ombudsman:** Create a dedicated wing within the Data Protection Board of India focused exclusively on processing child privacy complaints, conducting algorithmic transparency audits, and penalizing predatory developers.
- **Mandate Privacy Impact Assessments (PIA):** Obligate Data Fiduciaries whose platforms are accessed by minors to conduct mandatory yearly Privacy Impact Assessments focused on potential harms to children.

9. CONCLUSION

The digital privacy of young users stands at a critical legal, social, and technological crossroads. As India advances its vision of a digitally empowered society, it must ensure that children navigate online spaces without surrendering their fundamental constitutional rights

to privacy, autonomy, and human dignity.

While the enactment of the Digital Personal Data Protection Act, 2023 represents a major step forward, rigid statutory rules alone cannot keep pace with rapidly evolving technologies like generative AI, immersive virtual gaming, and intrusive micro-targeting algorithms. A comprehensive protective ecosystem demands a multi-pronged approach—combining flexible legislative frameworks, statutory Privacy-by-Design standards, robust regulatory oversight, and privacy-preserving age verification technologies. Protecting young users online is not merely about regulating code; it is about safeguarding the future of youth autonomy, safety, and democracy in India.

REFERENCES (BLUEBOOK CITATION STYLE)

1. CONSTITUTION OF INDIA, 1950, Arts. 14, 19(1)(a), 21, 39(f).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
3. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
4. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
5. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and Information Technology (India).
6. The Protection of Children from Sexual Offences (POCSO) Act, 2012, No. 32, Acts of Parliament, 2012 (India).
7. United Nations Convention on the Rights of the Child (UNCRC), Nov. 20, 1989, 1577 U.N.T.S. 3.
8. UNCRC General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (Mar. 2, 2021).
9. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (1998) (United States).
10. Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), Art. 8 & Art. 17, 2016 O.J. (L 119) 1.
11. Information Commissioner's Office (ICO), Age Appropriate Design: A Code of Practice for Online Services (United Kingdom, 2020).
12. NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll (2018).
13. Central Consumer Protection Authority (CCPA), Guidelines for Prevention and Regulation of Dark Patterns (2023) (India).
14. UNICEF, The State of the World's Children 2017: Children in a Digital World (2017).