

International Journal Research Publication Analysis

Page: 01-09

DIGITAL PRIVACY PROTECTION FOR YOUNG USERS

***Rajnandani Chaudhary**

S.Y. LL.B. College Name: Haveli Institute of Legal Studies and Research, Silvassa

(Affiliated to Mumbai University)

Article Received: 26 August 2026

Article Revised: 13 September 2026

Published on: 03 October 2026

***Corresponding Author: Rajnandani Chaudhary**

S.Y. LL.B. College Name: Haveli Institute of Legal Studies and Research, Silvassa

(Affiliated to Mumbai University)

DOI: <https://doi-doi.org/101555/ijrpa.2489>

ABSTRACT

Children and teenagers today spend a large part of their daily lives online — studying, playing games, chatting with friends, and scrolling through social media — often without fully understanding how much of their personal information is being collected, stored, and used in the process. This growing gap between how much time young users spend online and how little they understand about data privacy has made “digital privacy protection for young users” one of the most pressing legal and policy issues of our time. This paper examines the legal framework built around the protection of children’s personal data, with a particular focus on India’s Digital Personal Data Protection Act, 2023, along with its accompanying Rules of 2025, and situates this framework alongside comparable laws such as the Children’s Online Privacy Protection Act (COPPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. The paper studies the specific risks young users face online — targeted advertising, behavioural tracking, data breaches, and exposure to predatory actors — and evaluates how effectively current laws address these risks through mechanisms like verifiable parental consent, restrictions on tracking and profiling, and penalties for non-compliance. It also looks at relevant judicial pronouncements that have shaped the constitutional and legal understanding of privacy as a fundamental right in India, and how that understanding extends to children as a particularly vulnerable class of data principals. The paper concludes by identifying gaps that remain in the current legal architecture and offers practical suggestions — for lawmakers, platforms, schools, and parents — aimed at making the digital space genuinely safer for young users without cutting them off from the benefits of the internet.

KEYWORDS: Digital Privacy, Children’s Data Protection, Digital Personal Data Protection Act 2023, DPDP Rules 2025, Right to Privacy, Parental Consent, Data Fiduciary, COPPA, GDPR, Online Safety of Minors.

I. INTRODUCTION

The internet has become an inseparable part of growing up in the twenty-first century. Children as young as five or six now use tablets and smartphones for schoolwork, entertainment, and communication, while teenagers practically live on social media, gaming platforms, and messaging apps. This constant online presence generates an enormous trail of personal data — names, dates of birth, location, browsing habits, voice recordings, photographs, and even biometric data in some cases. Unlike adults, young users rarely read privacy policies, rarely question why an app wants access to their camera or contacts, and are far more likely to click “I agree” without a second thought, simply to get to the game or video they want to watch.

This creates a genuine legal problem. Personal data belonging to a person who cannot yet fully understand its value or its risks is, by definition, personal data that needs a different, more protective legal treatment than the data of a fully informed adult. Around the world, lawmakers have responded to this problem in different ways. The United States enacted the Children’s Online Privacy Protection Act (COPPA) as early as 1998, long before smartphones existed, specifically to regulate how websites collect data from children under thirteen. The European Union’s General Data Protection Regulation (GDPR), which came into force in 2018, introduced special conditions for children’s consent and required member states to set an age of digital consent between thirteen and sixteen. India, coming somewhat later to comprehensive data protection legislation, passed the Digital Personal Data Protection Act in August 2023, and followed it up with detailed operational rules in 2025 that specifically address how children’s data must be handled.

What makes this area of law particularly important right now is the sheer scale of the risk. Data breaches involving children’s information, predatory behaviour enabled by location-sharing features, and psychologically manipulative design features aimed at keeping young users engaged for longer (and therefore generating more data and more advertising revenue) have all become well-documented problems. At the same time, young users are not merely passive victims; they are also rights-holders under the Constitution, entitled to dignity, autonomy, and privacy, even if the exercise of some of those rights is necessarily mediated through a parent or guardian until they reach adulthood.

This paper examines how the law — particularly Indian law, read alongside relevant international frameworks — currently approaches the task of protecting young users’ digital privacy. It looks at the legal principles involved, the specific statutory mechanisms that have been put in place, the judicial background that supports treating privacy as a fundamental right, and the practical gaps that remain between what the law says and what actually happens to a child’s data online.

II. Research Methodology

This paper adopts a **doctrinal, qualitative research methodology**, relying on both primary and secondary legal sources. The research draws upon:

1. Primary legal sources — the Constitution of India, particularly Article 21; the Digital Personal Data Protection Act, 2023; the Digital Personal Data Protection Rules, 2025 (including Rule 10 on verifiable parental consent and Rule 11 on exemptions); the Information Technology Act, 2000, and its associated rules; and, for comparative purposes, the Children’s Online Privacy Protection Act (COPPA), 1998 (USA), and the General Data Protection Regulation (GDPR), 2016 (EU).

2. Judicial precedent — landmark decisions of the Supreme Court of India that establish and interpret the right to privacy as a fundamental right, most notably *Justice K.S. Puttaswamy (Retd.) v. Union of India*, which forms the constitutional foundation on which India’s data protection framework, including the protections for children, ultimately rests.

3. Government and regulatory material — official notifications and explanatory material issued by the Ministry of Electronics and Information Technology (MeitY) regarding the DPDP Rules, 2025, and publicly available guidance on compliance obligations relating to children’s data.

4. Secondary academic and policy literature — law firm analyses, policy commentary, and legal explainers examining how the DPDP Act and Rules operate in practice, along with comparative commentary on COPPA and GDPR.

The methodology is analytical and comparative rather than empirical. The paper does not conduct primary surveys of young users or platforms; instead, it critically examines the existing legal text, judicial reasoning, and policy commentary to build a coherent picture of how digital privacy protection for young users currently functions in India, and how it measures up against comparable international frameworks. The main limitation of this method is that it cannot measure real-world compliance or enforcement outcomes directly; it can only assess the legal architecture and the risks and gaps embedded within it.

III. Legal Analysis

A. The Constitutional Foundation: Privacy as a Fundamental Right

Before examining the specific statutory scheme, it is important to understand the constitutional basis on which any privacy protection for children in India rests. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Article 21 of the Constitution, as part of the right to life and personal liberty. The Court recognised informational privacy — control over the dissemination of one’s personal data — as a core element of this right. Although the case itself did not deal specifically with children, its reasoning has become the constitutional bedrock for all subsequent data protection legislation in India, including the protections extended to minors. If privacy is a fundamental right for every individual, then a child, as a rights-bearing citizen who simply lacks full legal capacity to exercise certain rights independently, is equally entitled to that protection — exercised, where necessary, through a parent or lawful guardian.

B. The Digital Personal Data Protection Act, 2023 — Section 9

The primary statutory provision dealing with children’s data in India is Section 9 of the DPDP Act, 2023. This section requires that before processing the personal data of a child, a data fiduciary (essentially, any organisation or platform that collects and uses personal data) must obtain verifiable consent from the child’s parent or lawful guardian. The Act defines a “child” as any individual below the age of eighteen years, a notably higher threshold than COPPA’s cut-off of thirteen years or GDPR’s flexible range of thirteen to sixteen years, depending on the member state.

Section 9 further prohibits data fiduciaries from undertaking any processing of a child’s data that is likely to cause a detrimental effect on the child’s well-being. It also places two specific and absolute restrictions on data fiduciaries: a prohibition on tracking or behavioural monitoring of children, and a prohibition on targeted advertising directed at children. These are significant provisions because they go directly after the two practices that are most commonly used by online platforms to keep users engaged and to monetise their attention — practices that are widely understood to be particularly harmful when directed at young, still-developing minds.

C. The DPDP Rules, 2025 — Operationalising the Protection

While Section 9 of the Act laid down the broad principle, it was the DPDP Rules, 2025, notified by the Ministry of Electronics and Information Technology, that gave these protections real operational teeth. Rule 10 of the DPDP Rules specifically deals with

verifiable consent for processing a child's personal data. It requires a data fiduciary to adopt appropriate technical and organisational measures to verify that the person identifying themselves as a parent is, in fact, an identifiable adult — for instance, by cross-referencing details already available with the data fiduciary, or through documents voluntarily provided via a Digital Locker service. This is a meaningful step beyond a simple “tick the box to confirm you are over eighteen” model, which has historically been very easy for children to bypass by simply lying about their age.

Rule 11 provides certain narrow exemptions from these obligations — for instance, for processing that is genuinely necessary for purposes such as healthcare, education, or the real-time safety of the child, or for certain categories of data fiduciaries such as educational institutions or child transport services, whose core function requires processing a child's data in ways that would otherwise be difficult to reconcile with strict parental-consent requirements at every step.

D. Penalties and Enforcement

The DPDP Act backs these obligations with substantial financial penalties. Non-compliance with obligations relating to children's data can attract penalties running up to ₹200 crore, one of the highest penalty brackets under the entire Act, reflecting how seriously the legislature has treated this category of harm. The Data Protection Board of India, established under the Act, is responsible for adjudicating breaches and imposing these penalties, giving the framework an institutional mechanism for enforcement rather than leaving it purely to civil litigation.

E. Comparative Perspective — COPPA and GDPR

Looking outside India, the United States' COPPA requires operators of websites and online services directed at children under thirteen to obtain verifiable parental consent before collecting personal information, and imposes similar restrictions on the use of that data for purposes like targeted advertising. COPPA's age threshold of thirteen has, however, been widely criticised as outdated, since it does not adequately protect teenagers aged thirteen to seventeen, who arguably face just as much risk from data-driven manipulation and profiling as younger children do.

The GDPR, applicable across the European Union, sets a “digital age of consent” that individual member states can fix anywhere between thirteen and sixteen years, below which parental consent is required for a child to lawfully use “information society services” involving data processing based on consent. The GDPR also embeds the broader principle of

“data protection by design and by default,” which, while not exclusively about children, has strong implications for how platforms likely to be used by young people should be built.

India’s approach, by setting the threshold at eighteen years and imposing both a consent requirement and outright prohibitions on tracking and targeted advertising, is in some ways more protective on paper than either of these frameworks. However, the practical challenge of verifying age and parental identity online — a problem that has troubled regulators everywhere — remains just as real in the Indian context as it does under COPPA or the GDPR.

F. Gaps Between Law and Practice

Despite this reasonably robust legal architecture, several practical gaps remain. First, age verification technology is still imperfect; a child can easily enter a false date of birth, and most platforms have no reliable way of confirming otherwise without collecting even more sensitive data, such as government identification, which raises its own privacy concerns. Second, much of the internet content that children access daily is hosted by global platforms whose primary compliance focus tends to be on larger markets like the United States and the European Union, which can create uneven or delayed compliance with India-specific requirements. Third, the DPDP framework primarily addresses data collected directly by data fiduciaries; it does not fully resolve the problem of children’s data being shared, scraped, or inferred by third parties, such as data brokers or advertising networks operating several steps removed from the original platform.

IV. Findings

1. India’s constitutional recognition of privacy as a fundamental right in *Puttaswamy* provides a strong doctrinal foundation for statutory protections of children’s data, even though the case itself did not directly concern minors.
2. Section 9 of the DPDP Act, 2023, sets one of the more protective legal thresholds globally by defining “child” as anyone below eighteen years and by prohibiting both behavioural tracking and targeted advertising directed at children, going further than COPPA’s narrower thirteen-year threshold.
3. The DPDP Rules, 2025, particularly Rule 10, meaningfully strengthen the consent framework by requiring verifiable identification of the consenting parent, moving beyond the largely symbolic “age gate” mechanisms that have proven easy for children to bypass in the past.

4. The penalty structure, with fines up to ₹200 crore for violations relating to children's data, signals that Indian lawmakers view harm to children's digital privacy as a serious regulatory concern, comparable in severity to major data breach violations.
5. Verifying age and parental identity online remains a genuine technical and practical challenge across all jurisdictions studied, including India, and represents the weakest link between the law as written and the law as actually enforced.
6. Comparative analysis shows that no single jurisdiction has fully solved the problem of protecting young users' privacy without either over-restricting their access to legitimate online services or under-protecting them from data-driven exploitation; each framework — Indian, American, and European — makes a different trade-off along this spectrum.

V. SUGGESTIONS

1. **Invest in privacy-preserving age-verification technology.** Rather than relying on children self-declaring their age or platforms demanding sensitive government identification, regulators and industry bodies should support the development of privacy-preserving verification methods that confirm a user is a minor without excessively collecting or storing additional personal data.
2. **Extend obligations more clearly to third-party data brokers and advertising networks.** The framework should be strengthened to ensure that entities several steps removed from the original data fiduciary — such as advertising networks that receive anonymised or pseudonymised data — remain within the scope of the child-data restrictions, closing a gap that current enforcement tends to overlook.
3. **Mandate simplified, child-friendly privacy notices.** Alongside the legal notice required for parental consent, platforms likely to be used by children should be required to provide a short, plain-language explanation aimed at the child themselves, so that even where consent is technically given by a parent, the child begins to understand what is happening to their data.
4. **Strengthen school-based digital literacy programmes.** Legal protection works best when paired with awareness. Schools should be encouraged, possibly through a formal curriculum requirement, to teach students not just how to use the internet, but how their personal data is collected, used, and potentially misused.
5. **Encourage periodic compliance audits specifically focused on children's data.** The Data Protection Board of India could prioritise proactive audits of platforms with a substantial young user base, rather than relying solely on complaint-driven enforcement,

given how unlikely it is that a child or even a parent would recognise a subtle violation such as covert behavioural tracking.

6. Review the eighteen-year threshold for graduated consent. A single threshold treats a six-year-old and a seventeen-year-old identically in terms of requiring parental consent, which may not reflect the practical reality of how older teenagers use the internet independently. A graduated model, similar in spirit to the flexibility seen under the GDPR, could allow older teenagers a degree of independent digital agency while retaining stronger protections for younger children.

VI. CONCLUSION

Digital privacy protection for young users sits at an important intersection of constitutional rights, technology regulation, and everyday parenting. India's legal framework, built on the constitutional foundation laid in *Puttaswamy* and given detailed shape through the Digital Personal Data Protection Act, 2023, and its 2025 Rules, represents a genuinely serious legislative attempt to address this problem — arguably setting a higher formal standard of protection than comparable laws like COPPA in the United States, and in some respects matching the ambition of the GDPR in the European Union. The requirement of verifiable parental consent, the outright prohibition on tracking and targeted advertising directed at children, and the substantial penalties for non-compliance together create a framework that, if properly enforced, could meaningfully reduce the digital risks young users face today.

At the same time, the law on paper is only as strong as its practical enforcement. Age verification remains technically difficult, third-party data flows remain hard to fully regulate, and awareness among both children and parents about what these protections actually mean in daily life remains limited. Closing these gaps will require not just stronger rules, but sustained investment in better verification technology, clearer communication aimed at children themselves, and a regulatory posture that is proactive rather than merely reactive. Ultimately, protecting the digital privacy of young users is not a problem that law alone can solve — but a well-designed, well-enforced legal framework, of the kind India has begun to build, is an essential and overdue starting point.

REFERENCES

1. Constitution of India, 1950, art. 21.
2. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), s. 9.

3. Digital Personal Data Protection Rules, 2025, Rules 10 and 11, Ministry of Electronics and Information Technology, Government of India.
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
5. Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (1998), United States.
6. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, art. 8.
7. Information Technology Act, 2000, and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
8. Ministry of Electronics and Information Technology, Government of India, “Digital Personal Data Protection Rules, 2025 — Notification and Explanatory Guidance,” 2025.
9. CookieYes, “India Digital Personal Data Protection Act (DPDPA 2025): Updated Guide,” 2025.
10. EY India, “Transforming Data Privacy: DPDP Act, 2023 and DPDP Rules, 2025,” 2025.
11. Lawrbit, “DPDP Rules 2025: Understand India’s Data Protection Laws,” 2025.
12. Law.asia, “Indian Perspective on Protecting Children’s Personal Data,” 2024.
13. DPDPA.com, “Rule 10 of DPDP Rules 2025 — Verifiable Consent for Processing of Personal Data of Child,” Legal Interpretation Series.
14. DPDPA.com, “Comprehensive Legal Interpretation of Section 9 of the Digital Personal Data Protection Act, 2023.”