International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Children's Privacy under the Digital Personal Data Protection (DPDP) Act 2023: Adequate Protection or Regulatory Challenge?

Aayushi Meena[a]

[a]National Law Institute University, Bhopal, India

Received 25 April 2026; Accepted 25 May 2026; Published 28 May 2026

The rapid growth of digital technologies has significantly increased children's participation in online environments, exposing them to risks such as data exploitation, behavioural tracking, cyberbullying, identity theft, and privacy violations. Children often lack the awareness and maturity required to understand how their personal information is collected, processed, and used by digital platforms. In response to these concerns, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), establishing a comprehensive framework for regulating digital personal data and providing special safeguards for children. This article examines the legal framework governing children's data privacy under the DPDP Act, focusing on provisions relating to parental consent, restrictions on behavioural tracking, and protection against targeted advertisements. It further analyses implementation challenges, including age-verification difficulties, digital illiteracy, weak enforcement mechanisms, and cross-border data processing. The study concludes that while the DPDP Act is a significant step forward, stronger enforcement, awareness, and regulatory reforms remain essential.

Keywords: *data privacy, parental consent, behavioural tracking, informational privacy.*

INTRODUCTION

"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet."

— Gary Kovacs

In today's world, digital technology has become an inseparable part of human life. Adults now depend heavily on mobile phones, social media platforms, online shopping apps, digital payment systems, and internet-based services for their daily activities. Whether it is communication, education, entertainment, banking, or professional work, almost every aspect of life has shifted towards the digital world. This growing dependence on technology has not only changed the lives of adults but has also directly influenced the lifestyle of children.

Children today are introduced to smartphones, tablets, social media apps, gaming platforms, and online videos from a very young age. Earlier, childhood was mostly limited to classrooms, playgrounds, books, and physical interaction. However, in the modern era, a significant part of children's lives exists online. From attending virtual classes and watching educational videos to playing online games and using social networking platforms, children are now deeply connected with digital technology.

The problem, however, is that most children enter the digital world without fully understanding how it actually works. They do not understand concepts such as privacy, data collection, online tracking, or digital security. Whenever a child downloads a gaming application or creates an account on a social media platform, the application often asks for various types of information, such as name, age, photographs, email address, contact number, location access, microphone access, and camera permissions. Most children simply click on "Allow" or "Accept" without understanding why such information is being collected or how it may later be used.

For example, a child downloading an online game may unknowingly allow access to location services, photographs, contacts, or microphone permissions only to start the game quickly. Similarly, many online platforms encourage children to make in-app purchases through attractive advertisements and reward systems. In situations where parents' bank accounts or payment methods are linked with the device, money may automatically be deducted without proper awareness or consent. Such incidents have become increasingly common in recent years.

Apart from financial risks, children's online activities are continuously monitored through tracking systems and algorithms. Digital platforms often collect information regarding what children watch, search, like, or play online. This information is then used to show targeted advertisements and recommended content designed to increase screen time and user engagement. As a result, children's privacy, personal choices, and even location information are constantly exposed in the digital environment.

The increasing digital presence of children has therefore created serious concerns regarding online safety, misuse of personal information, behavioural manipulation, cyberbullying, identity theft, and invasion of privacy. Children are among the most vulnerable users of the internet because they lack the maturity to understand the long-term consequences of sharing personal information online.

Recognising these growing concerns, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act)[1], to regulate the collection and processing of digital personal data and to protect the privacy rights of individuals, especially children. The Act introduces safeguards such as parental consent, restrictions on tracking, and limitations on targeted advertisements directed towards minors. However, despite these protections, several practical and legal challenges still remain. This article examines the issue of children's privacy under the Digital Personal Data Protection Act, 2023 and analyses whether the law is capable of adequately protecting children in today's rapidly evolving digital world.

WHY CHILDREN'S DATA PRIVACY MATTERS

As discussed above, Children are among the most active users of the internet today. This makes them vulnerable to exploitation, manipulation, and misuse of personal data. Children possess the same constitutional rights to dignity, autonomy, and informational privacy as adults. Therefore, protecting children's data is not merely a regulatory concern but also a constitutional obligation. The following are some major effects and concerns related to children's data privacy, discussed in detail for a better understanding of this issue:

Risk of Online Exploitation: When children share personal information online, they may become vulnerable to identity theft, cyberbullying, online predators, fraud, stalking, and

[1] Digital Personal Data Protection Act 2023

emotional manipulation. For example, if a gaming app collects location information and personal details of a child, such information may be misused if adequate safeguards are not maintained.

Behavioural Tracking and Manipulation: Modern digital platforms operate through algorithms that study user behaviour. Companies track what users watch, search, like, and purchase online. This information is used to influence future choices and increase engagement. Children are especially vulnerable to such systems because they can be easily attracted by online advertisements and recommendations. For instance, if a child watches toy videos repeatedly, the platform may continuously show toy advertisements or similar content. Over time, this may affect the child's behaviour, spending habits, and mental health.

Long-Term Digital Footprints: Information shared online often remains permanently available. Children may upload photographs, videos, or comments without realising that such information can stay online for years. This creates long-term digital footprints that may affect future opportunities, reputation, and personal privacy.

Mental and Emotional Impact: Excessive digital monitoring and online targeting can negatively affect children's emotional development. Social media pressure, harmful content, and manipulative advertisements may lead to anxiety, low self-esteem, addiction, and mental stress. Therefore, protecting children's privacy is not only a technological issue but also a social and psychological necessity.

Privacy as a Constitutional Value: The right to privacy is closely connected with dignity and liberty. Children also possess constitutional rights to dignity, autonomy, and privacy. Therefore, protecting their personal data becomes a constitutional responsibility.

Concerns Regarding Educational Applications: Many educational technology platforms collect learning patterns, attendance records, behavioural information, and engagement metrics of children. Critics argue that insufficient regulation may expose children to profiling and commercialisation. This became more visible during the COVID-19 pandemic when online learning increased rapidly.

In conclusion, the growing digital presence of children has increased the risks discussed above. Therefore, there is a strong need for effective legal protection to safeguard children in the digital

environment. The enactment of the Digital Personal Data Protection Act, 2023, is an important step towards ensuring safer collection, storage, and use of children's personal data in India.

OVERVIEW OF THE DPDP ACT, 2023

The Digital Personal Data Protection Act, 2023, is India's first comprehensive law made to protect the personal data of individuals in the digital environment. The Act regulates how companies, websites, applications, and organisations collect, store, use, and process personal data. It gives individuals certain rights over their personal information and places responsibilities on entities that collect data.

The Act also gives special protection to children by requiring parental consent before collecting children's data and restricting harmful tracking or targeted advertisements directed at them. Overall, the law aims to ensure privacy, transparency, and safer use of personal data in the digital age. The Digital Personal Data Protection Act, 2023, was further operationalised and supplemented through the DPDP Rules, 2025.[2] These Rules were notified by the Ministry of Electronics and Information Technology (MeitY) to explain how the Act would actually function in practice.

HISTORY AND DEVELOPMENT OF THE DPDP ACT, 2023

For many years, India did not have a dedicated and comprehensive law specifically dealing with data protection and privacy. Earlier, issues relating to digital privacy and protection of online information were mainly governed by the Information Technology Act, 2000 and certain rules framed under it, particularly the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[3] However, these provisions were considered limited because they were introduced at a time when India's digital ecosystem was still developing.

Over the years, rapid technological growth transformed the manner in which people interacted with digital platforms. Social media applications, e-commerce websites, digital payment systems, online gaming platforms, educational technology applications, and artificial

[2] Digital Personal Data Protection Rules 2025
[3] Information Technology Act 2000; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

intelligence systems began collecting massive amounts of personal information from users. Children, who increasingly became active internet users, also started sharing personal information online without understanding the consequences of such disclosure.

At the same time, concerns regarding online surveillance, data breaches, unauthorised sharing of information, identity theft, behavioural tracking, targeted advertisements, and misuse of personal data started increasing across the world, as well as in India. The absence of a strong data protection law created serious legal and constitutional concerns regarding privacy and informational autonomy.

The demand for a comprehensive privacy framework became much stronger after the landmark judgment of Justice K.S. Puttaswamy v Union of India.[4] In this case, 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 of India.[5] The Court observed that privacy is closely connected with dignity, liberty, autonomy, and informational self-determination. The judgment highlighted the growing importance of informational privacy in the digital age and recognised the need for stronger legal safeguards against misuse of personal data.

Following this judgment, the Government of India constituted the Justice B.N. Srikrishna Committee in 2017 to examine issues relating to data protection and recommend a legal framework for India.

The Committee submitted a detailed report, policy recommendations, and a draft Personal Data Protection Bill.[6]

The proposed framework was heavily influenced by international privacy models, especially the General Data Protection Regulation (GDPR),[7] which is considered one of the strongest data protection frameworks in the world.

Several versions of the proposed legislation were introduced over time:

[4] *Justice K S Puttaswamy & Anr v Union of India & Ors* (2017) 10 SCC 1
[5] Constitution of India 1950, art 21
[6] The Committee of Experts on a Data Protection Framework for India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)
[7] General Data Protection Regulation 2016

- Personal Data Protection Bill 2018,
- Personal Data Protection Bill 2019,
- Digital Personal Data Protection Bill 2022,
- and finally, the Digital Personal Data Protection Act, 2023.

The DPDP Act[8] was enacted in August 2023 with the objective of creating a comprehensive framework regulating the collection, storage, processing, and transfer of digital personal data in India.

The primary objectives of the Act include:

- Protection of personal data,
- Regulation of data processing,
- Accountability of organisations handling data,
- Prevention of misuse of personal information, and
- Protection of the privacy rights of individuals.

The legislation is especially important because it specifically recognises children as vulnerable users requiring additional protection in digital environments. However, although the DPDP Act, 2023, established the legal framework, many practical aspects regarding implementation, compliance procedures, consent mechanisms, grievance redressal, and enforcement were still unclear. Therefore, the Government later introduced the DPDP Rules 2025[9] to operationalise and implement the provisions of the Act effectively.

The DPDP Rules 2025 play an important role because they provide procedural clarity regarding:

- Consent notices,
- Parental consent verification,
- Data breach reporting,
- Cybersecurity obligations,
- Grievance redressal systems, and
- The Functioning of the Data Protection Board of India.

[8] Digital Personal Data Protection Act 2023
[9] Digital Personal Data Protection Rules 2025

One of the most significant aspects of the DPDP Rules, 2025 relating to children is the strengthening of "verifiable parental consent." The Rules require Data Fiduciaries to adopt appropriate technical and organisational measures to verify that consent for processing children's data is genuinely provided by parents or lawful guardians.

Rule 10 of the DPDP Rules, 2025 states: "A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child."[10]

The Rules also continue the prohibition on behavioural tracking of children, targeted advertisements directed towards minors, and harmful processing of children's personal data.

The DPDP Rules, 2025, further emphasise the importance of simple and transparent consent notices. Instead of complicated privacy policies filled with technical language, companies are expected to provide notices in clear and understandable language so that users, including parents, can better understand how personal information is being processed.

Another important feature introduced through the 2025 Rules relates to personal data breaches. In case of a data breach, organisations are required to inform affected individuals, explain the nature of the breach, identify the type of information affected, and disclose remedial measures being taken. The Rules also strengthen accountability obligations of Data Fiduciaries by requiring: stronger security safeguards, responsible data handling practices, limited data collection, and protection against unauthorised access. Nevertheless, the enactment of the DPDP Act and the subsequent introduction of the DPDP Rules, 2025 mark a significant step towards recognising privacy as an essential right in the digital age, particularly for children who are among the most vulnerable participants in today's online ecosystem.

IMPORTANT DEFINITIONS UNDER THE DPDP ACT.

Digital personal data means personal data in digital form.

[10] *Ibid* r 10

Personal data: Personal data means any data about an individual who is identifiable by or in relation to such data. Examples are name, phone number, email address, photographs, location information, browsing history, biometric information, etc.

Child: Under the DPDP Act, a child means any person below eighteen years of age. This definition is important because special protections under the law apply to individuals below eighteen.

Data Fiduciary: A Data Fiduciary is any person, company, organisation, or government body that determines the purpose and means of processing of personal data. Examples include social media companies, gaming applications, educational platforms, e-commerce websites, and online learning apps.

Data Principal: A Data Principal refers to the individual to whom the personal data relates, and where such individual is

(i) a child, includes the parents or lawful guardian of such a child;

(ii) a person with disability, including her lawful guardian, acting on her behalf.

Data Processing: Data processing includes any activity involving personal data, such as collection, storage, sharing, etc.

Privacy: Privacy refers to the right of individuals to control their personal information and protect their personal space and autonomy.

Data Protection: Data protection means safeguarding personal information from misuse, unauthorised access, exploitation, and illegal disclosure.

Personal data breach: means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

MAIN FEATURES, FUNCTIONS AND IMPORTANCE OF THE DPDP ACT

The DPDP Act creates a framework for regulating digital personal data in India.

Consent-Based System: The law is mainly based on consent. Before collecting or processing personal data, companies must obtain valid consent from individuals. Consent must be free, informed, specific, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of the personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. This means users should understand what information is being collected, why it is being collected, and how it will be used.

Example**:** Suppose an online learning application wants access to a child's camera and microphone. The company must clearly explain why such access is required before collecting the information.

Verifiable Parental Consent: One of the most important child-related provisions under the Act is the requirement of verifiable parental consent. Before processing a child's personal data, Data Fiduciaries must obtain consent from parents or lawful guardians.

Example: If a thirteen-year-old child wants to create an account on a gaming application, the company must first verify parental permission. The purpose of this provision is to ensure that children are protected from harmful digital practices.

Restriction on Behavioural Tracking: The Act prohibits tracking children online, behavioural monitoring, and targeted advertising directed toward minors. This is important because many digital companies use algorithms to study user behaviour and increase engagement. Children are particularly vulnerable to manipulation through such systems.

Example**:** If a child repeatedly searches for cartoons or games, platforms should not continuously use that information to target addictive advertisements.

Rights of Individuals: The Act grants several rights to Data Principals. These include the right to access personal data, the right to correction of inaccurate data, the right to erasure, and the right to grievance redressal. These rights give individuals greater control over their information.

EXISTING PROBLEMS RELATING TO DATA PRIVACY

Even though legal frameworks are developing, several practical problems continue to exist.

Excessive Data Collection: Many applications collect more information than necessary. For example, gaming apps demanding microphone permissions, and educational apps tracking behaviour patterns. This increases the risk of misuse.

Lack of Awareness: Most people do not fully understand privacy policies, terms and conditions, tracking systems, or data-sharing practices. Children are even less likely to understand such issues. As a result, consent often becomes a mere formality.

Weak Cybersecurity Systems: Data breaches are becoming increasingly common. Personal information may be leaked due to hacking, poor security systems, employee negligence, or unauthorised sharing. Once leaked, personal data may be difficult to recover or protect.

Manipulative Algorithms: Digital platforms use algorithms to influence user behaviour. Children are especially vulnerable because they may spend excessive time online without understanding how recommendation systems work. This may increase addiction, emotional dependency, impulsive purchasing, and exposure to harmful content.

REAL-LIFE CASE EXAMPLES RELATING TO DATA PRIVACY

Cambridge Analytica-Facebook Scandal: One of the most famous global privacy controversies involved Facebook and Cambridge Analytica. Personal information of millions of Facebook users was collected without proper consent and used for political advertising purposes. The incident demonstrated how personal data can be misused to influence behaviour and opinions. Although the case mainly involved adults, it highlighted larger concerns regarding user privacy and misuse of digital information.

WhatsApp Privacy Policy Controversy: WhatsApp faced criticism after changes to its privacy policy relating to data sharing with its parent company, Meta. Users expressed concerns regarding a lack of informed consent, excessive data collection, and monopolistic control over user information. The controversy became significant in India due to the large number of young users on the platform.

INDIAN SCENARIO: CURRENT POSITION AND CHALLENGES

India is one of the largest digital markets in the world. Affordable internet services and smartphone access have significantly increased internet usage among children. However, India also faces serious challenges in implementing strong data privacy protections.

Uniform Age Threshold: One major criticism concerns the Act's uniform age threshold of eighteen years. Critics argue that treating a seventeen-year-old and a young child identically fails to recognise the evolving capacity and digital understanding of adolescents. In several jurisdictions, such as the European Union, teenagers above a specified age may independently consent to certain online services.

Difficulties in Verifying Parental Consent: Another significant challenge concerns the implementation of verifiable parental consent. In practice, companies may find it difficult to accurately verify whether consent has genuinely been provided by a parent or guardian. Children may bypass restrictions by providing false information, using fake ages, or accessing accounts through third parties. Consequently, enforcement of the provision becomes complicated.

Digital Illiteracy: Many parents and children are not aware of online privacy settings, digital risks, or methods of protecting personal information. This lack of awareness increases vulnerability.

Weak Enforcement Mechanisms: India still faces a lack of cyber infrastructure, limited digital literacy, a shortage of cyber experts, and inadequate enforcement mechanisms for digital forensic systems. Without effective implementation, legislative safeguards may remain merely symbolic.

Rapid Expansion of Digital Platforms: The use of gaming applications, social media, online learning platforms, and AI-based services has increased rapidly. This creates greater opportunities for data collection and behavioural monitoring.

Cross-Border Data Processing: Many digital companies store and process data outside India. This creates difficulties relating to jurisdiction, enforcement, and accountability.

There should be implementation of better age-verification systems, simpler privacy policies, stricter punishment for misuse, stronger regulation of EdTech/gaming apps, awareness for parents and children, and separate rules for teenagers.

Although the DPDP Act represents an important step toward recognising children's digital privacy rights, further reforms are necessary. India should consider adopting flexible age-based consent systems, creating stronger age-verification mechanisms, introducing child-friendly privacy policies, strengthening cyber enforcement infrastructure, increasing digital literacy among parents and children, and imposing stricter accountability upon platforms targeting minors. As stated by Sundar Pichai, "Privacy cannot be a luxury good." This statement reflects the idea that digital privacy must remain accessible and protected for every individual, including children.

COMPARISON & LEARNING FROM OTHER COUNTRIES

European Union – GDPR: The European Union's General Data Protection Regulation (GDPR)[11] is considered one of the strongest privacy frameworks in the world. The GDPR provides strong consent requirements, the right to be forgotten, data portability, and child-specific safeguards. Under the GDPR, member states may fix the age of consent between thirteen and sixteen years. Compared to the GDPR, India's eighteen-year threshold is stricter.

United States – COPPA: The United States enacted the Children's Online Privacy Protection Act (COPPA).[12] The law protects children below thirteen years of age. Websites directed toward children must: obtain parental consent, disclose privacy policies, and maintain security measures. Unlike India's broader law, COPPA specifically focuses on children's online privacy.

United Kingdom – Age-Appropriate Design Code: The United Kingdom introduced the Age-Appropriate Design Code.[13] The framework requires online platforms to prioritise children's privacy and welfare while designing digital services. The system focuses on privacy-friendly settings, reduced tracking, and child safety.

[11] General Data Protection Regulation 2016
[12] Children's Online Privacy Protection Act 1998
[13] *Age appropriate design: a code of practice for online services* (Information Commissioner's Office 2021)

UNDERSTANDING THE TOPIC AS A LAW STUDENT

Studying children's privacy under the DPDP Act shows how the law is evolving alongside technology. Earlier, legal systems mainly focused on physical crimes and traditional disputes. Today, personal data itself has become a valuable economic resource. This topic demonstrates that privacy is no longer limited to physical space. It now includes digital identity, online behaviour, and informational autonomy. The DPDP Act reflects India's attempt to balance technological innovation, economic growth, business interests, and constitutional rights. However, studying the Act also reveals that passing legislation alone is not enough. Effective protection requires: digital awareness, strong enforcement, responsible technology companies, and active participation by parents and educational institutions. The debate surrounding children's privacy also raises larger constitutional and ethical questions: Should teenagers have limited digital autonomy? How should the law regulate artificial intelligence and algorithms? Can privacy survive in a data-driven economy? How can the law balance innovation and individual rights? These questions indicate that privacy law will continue to develop rapidly in the future. As law students, understanding such developments is important because technology-related legal issues will become increasingly significant in legal practice and policymaking.

CONCLUSION

The Digital Personal Data Protection Act, 2023, represents a major step in India's effort to create a comprehensive privacy framework in the digital age. The law recognises that children are vulnerable users who require special protection online. Provisions relating to parental consent, restrictions on tracking, and limitations on targeted advertisements show the legislature's intention to protect children's dignity and informational privacy. At the same time, several practical challenges continue to exist. Weak enforcement systems, lack of digital awareness, broad governmental exemptions, and difficulties relating to parental consent create concerns regarding the effectiveness of the framework. The law also raises important questions regarding teenage autonomy and the balance between protection and freedom. Protecting children's privacy cannot depend only upon legislation. It requires cooperation among government authorities, parents, schools, technology companies, and society.

Digital awareness and responsible online practices are equally important. As technology continues to evolve rapidly, India's legal framework must also evolve to address new challenges

involving artificial intelligence, behavioural tracking, and digital surveillance. Ultimately, protecting children's data is not merely about regulating technology. It is about protecting dignity, freedom, autonomy, and the future of the next generation.

"The right to privacy is the right to protect one's individuality."

— Dr A.P.J. Abdul Kalam