International Journal of Science, Strategic Management and Technology
Volume **02** Issue **06** June-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

"Legal Protection of Children's Data in the Digital Age: An Analysis of the DPDP Act, 2023"

Adv. Jyoti Sawant LL.M. (Cyber Law)

jyotisawant309@gmail.com

Bharati Vidyapeeth (Deemed to Be University) New Law College, Pune

https://doi.org/ 10.55041/ijsmt.v2i6.130

Cite this Article: LL.M., A. J. S. (2026). "Legal Protection of Children's Data in the Digital Age: An Analysis of the DPDP Act, 2023". International Journal of Science, Strategic Management and Technology, *02*(6). https://doi.org/10.55041/ijsmt.v2i6.130

ABSTRACT

The swift advancement of digital technologies has revolutionized how people communicate, learn, interact, and obtain information. Children, in particular, have become active participants in the digital world through social media, online gaming, educational technology, streaming services, and AI-based tools. In India, the recognition of privacy as a fundamental right in the case of Justice K.S. Puttaswamy v. Union of India established the constitutional basis for data protection laws. In response to increasing concerns about digital privacy, the Parliament passed the Digital Personal Data Protection Act, 2023 (DPDP Act), marking India's first comprehensive legislation on digital personal data. The Act includes specific protections for children by requiring verifiable parental consent and banning tracking, behavioral monitoring, and targeted advertising aimed at minors. This Article critically explores the legal framework for protecting children's personal data under the DPDP Act, 2023. The study examines the constitutional foundation of privacy, the development of data protection laws, and the child-specific provisions in the Act. It also assesses the effectiveness of the current framework by identifying practical challenges such as age verification issues, implementation obstacles, lack of digital literacy, regulatory ambiguities, and enforcement concerns. The research further conducts a comparative analysis of international frameworks like the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA).

1. INTRODUCTION

In today's era, technology is everywhere. It's completely changed how we talk to each other, & learn new things, run businesses, and socialize. These days, we rely so much on the internet, smartphones, social media, digital education tools, gaming apps, and all kinds of online entertainment. Because of that, companies are collecting large amounts of personal data, storing it, processing it, sharing it, you name it. While this makes life more connected and simpler, it also raises anxiety about privacy and keeping personal information safe & secure, especially for kids. Children are right in the middle of this digital world they use educational apps, social media, video-sharing sites, games, learning platforms, smart watches, even AI-driven services all before they can really understand what's happening with their information. All that activity means their personal details like who they are, how they behave, what sites they visit, where

they go, even their call logs and biometric info which are private are constantly being collected and let's be honest, children just don't have the mental development or legal awareness to fully grasp what digital consent means or how privacy policies work. They can't see all the ways their data gets used, or misused, by algorithms or advertisers. That leaves them wide open to all kinds of risks: data misuse, profiling, manipulation, surveillance, targeted ads, identity theft, cyber exploitation & the list goes on.Even with these safeguards & protection, numerous legal, technological, and practical challenges remain unaddressed. Furthermore, the Act does not provide clear guidance on practical age verification methods, the responsibilities of digital intermediaries, the exemptions allowed for certain organizations, or the enforcement framework. Other issues include algorithmic profiling, deceptive digital design practices, cross-border data handling, and the commercial use of children's behavioral data by major internet companies. This legal analysis of the framework that oversees the DPDP ACT, 2023. It highlights both legal and practical application shortcomings, assesses the sufficiency of current legal protections, and suggests reforms to enhance India data secure of children.

Children in the Digital Ecosystem

In today's world, children are key players in the digital landscape. Unlike past generations, modern children are raised in settings where digital interaction is integral to their education, play, communication, social interactions, and identity development from a young age. The digital realm is no longer separate from childhood; it has become an essential component of it.

Children interact with digital ecosystems in various ways, such as:

(i) Educational Platforms

Digital classrooms, learning management systems, tutoring apps, exam portals, and AI-driven educational tools gather a wealth of student data, including: identity information; academic achievements; attendance trends; learning preferences; performance metrics; behavioral indicators; communication records; and device usage statistics. Educational technology platforms often claim that data collection is crucial for personalization and enhancing learning outcomes. However, concerns arise when educational data is commercially analyzed or used beyond educational purposes.

(ii) Social Media Platforms

Teenagers and increasingly younger children use social networking sites for communication, self-expression, entertainment, and social validation. These platforms gather: personal identifiers; photos and videos; friend networks; messaging habits; interests; engagement patterns; location data; inferred psychological profiles. Algorithmic recommendation systems can greatly influence children's attention, perspectives, and behavioral development.

(iii) Online Gaming Ecosystems

Gaming platforms collect extensive behavioral and transactional data, including: gameplay habits; reaction times; in-game purchases; communication patterns; reward sensitivity; social interaction data; attention cycles; emotional engagement patterns. Children are particularly susceptible to persuasive monetization strategies embedded in gaming structures.

(iv) Video-Sharing and Entertainment Platforms

Children are increasingly consuming content through algorithmically curated streaming services. Viewing history, watch duration, emotional response indicators, content preferences, and interaction behavior become valuable data assets used for predictive recommendations and advertising.

(v) Smart Devices and Connected Technology

Wearables, smart toys, voice assistants, and connected educational devices collect: voice recordings; movement data; health indicators; location data; biometric signals; behavioural analytics. This extends data collection from screen-based activities to the physical and intimate aspects of children's lives.

Digital Childhood and Identity Formation

A significant aspect of digital childhood is that identity development is increasingly taking place within data-centric environments. Elements such as social validation, communication methods, educational achievements, entertainment choices, and self-representation are often facilitated by digital platforms. As a result, privacy issues impacting children extend beyond mere information they can influence psychological growth, independence, emotional health, and social development. Children's engagement in digital spaces also leads to enduring digital footprints, which can be accessed or analyzed over extended periods. Therefore, children within digital ecosystems are not just users they are constant data producers, subjects of profiling, targets for commercial interests, and participants in environments crafted through advanced behavioral engineering[1].

Vulnerability of Children's Data

The susceptibility of children's personal data stems from the convergence of developmental immaturity, informational imbalance, commercial exploitation, technological intricacy, and insufficient regulatory protections. Children need enhanced legal safeguards because the risks associated with data processing are heightened for them.

(i) Limited Capacity for Informed Consent

Children often lack the cognitive maturity to comprehend: privacy policies; consent frameworks; data collection methods; long-term implications of sharing information; profiling and algorithmic impacts. As a result, consent obtained from children is frequently formal rather than truly informed.

(ii) Susceptibility to Manipulation

Children are more easily swayed by: persuasive interface designs; reward mechanisms; nudging strategies, emotional targeting; personalised advertisements; influencer marketing; gamified engagement loops. Behavioral data allows for increasingly precise manipulation.

(iii) Long-Term Profiling Risks

Profiling during childhood can establish enduring behavioral models that affect future: educational prospects; commercial targeting; reputation; social identity; algorithmic categorization. A digital record created in childhood may follow into adulthood.

(iv) Safety Risks

Unauthorized access to children's personal data can expose them to: cyber exploitation; identity theft; stalking; location tracking; grooming threats; financial fraud targeting families.

(v) Psychological Harm

[1] Starks, A., & Reich, S. M. (2024). Children's sensemaking of algorithms and data flows across YouTube and social media. *Information and Learning Sciences*, *125*(9), 673–692. https://doi.org/10.1108/ils-12-2023-0201

Ongoing surveillance and algorithmic interaction can impact: concentration; self-esteem; emotional regulation; social behavior; independent thinking; developmental freedom.

(vi) Dependence on Adults

Children's privacy rights are often mediated through parental consent, yet parents themselves may lack digital literacy or awareness of platform practices, creating protective gaps. For these reasons, protecting children's data should be viewed not just as regulatory compliance but as a matter of child welfare, dignity, developmental autonomy, and constitutional justice.

Constitutional Basis of Privacy in India

The constitutional foundation of privacy in India marks a pivotal advancement in contemporary Indian legal thought. While the Indian Constitution does not explicitly list privacy as a distinct fundamental right, judicial interpretations have gradually broadened the scope of constitutional rights to acknowledge privacy as essential to dignity, liberty, autonomy, and personal freedom. The evolution of privacy within the constitutional framework illustrates the shift in Indian constitutional law from a limited formal interpretation of rights to a more expansive human rights-focused perspective on liberty as outlined in Part III of the Constitution. At its core, privacy in India finds constitutional backing through the combined interpretation of Article 14, Article 19, and Article 21 of the Constitution.

Article 14, which ensures equality before the law and equal protection under the law, is pertinent to privacy discussions because arbitrary or biased handling of personal data can breach principles of substantive equality. Systems that rely on data for decision-making might perpetuate discrimination through profiling, exclusionary algorithms, or unclear digital classifications, thus raising constitutional issues related to fairness and equality.

Article 19, which safeguards freedoms such as speech, expression, movement, association, and profession, also has a privacy aspect. Exercising constitutional freedoms often requires a private space free from surveillance, coercion, or chilling effects. Individuals cannot freely think, communicate, associate, or express themselves if they are constantly monitored. Therefore, informational privacy is crucial for the meaningful exercise of democratic freedoms.

Article 21, which guarantees that no person shall be deprived of life or personal liberty except according to the procedure established by law, has become the main constitutional source of privacy rights. Privacy is thus seen as essential to meaningful human existence rather than a peripheral legal interest.

These constitutional standards now influence Indian data protection law. For children, the constitutional foundation of privacy is even more significant. Children are rights-bearing constitutional individuals entitled to dignity, liberty, equality, developmental autonomy, and protection against exploitation. Their vulnerability imposes a heightened constitutional duty on the State to ensure that digital environments do not compromise their welfare, freedom, or personality development. Thus, children's digital privacy is not merely a statutory issue it is fundamentally a constitutional concern[2].

Evolution from the IT Regime to the Digital Personal Data Protection Act, 2023

[2] Joshi, P., & Wamankar, Y. (2025). ALGORITHMIC POLICING AND DUE PROCESS IN CYBERCRIME INVESTIGATIONS: A CONSTITUTIONAL ANALYSIS UNDER ARTICLES 14, 19 AND 21 OF THE INDIAN CONSTITUTION. *ShodhSamajik: Journal of Social Studies*, *2*(2), 153–167. https://doi.org/10.29121/shodhsamajik.v2.i2.2025.57

Before the establishment of comprehensive data protection laws, India mainly depended on the Information Technology Act of 2000 and its related regulations to oversee certain elements of electronic data and cyber governance. The primary goals of the Information Technology Act were to acknowledge electronic records, support e-commerce, manage cyber crimes, and give legal validity to digital signatures. However, safeguarding privacy was not its main focus. Subsequent amendments added measures addressing unauthorized access, data theft, breaches of computer security, and offered limited compensation for the careless handling of sensitive personal data. The Sensitive Personal Data Rules aimed to control how corporations managed specific types of sensitive information by mandating privacy policies, consent, and reasonable security measures. Nonetheless, this framework had significant shortcomings, including a limited scope, weak enforcement, fragmented compliance, restricted individual rights, a lack of a comprehensive accountability structure, and insufficient protection against profiling and commercial exploitation. The rapid pace of digitalization highlighted the need for comprehensive legislation. After considering expert committee reports, draft bills, and policy discussions, India eventually passed the Digital Personal Data Protection Act, 2023. This act established a consent-based framework for managing digital personal data processing, defined the rights of data principals, outlined the responsibilities of data fiduciaries, and included protections specific to children. This development signified India's shift from fragmented cyber regulation to a more comprehensive approach to digital privacy governance[3].

Child Privacy Developments in India

The development of child privacy protection in India has traditionally been indirect and fragmented, primarily integrated within broader constitutional rights, child welfare laws, and cyber regulations, rather than through a specific child data protection framework. Historically, child protection laws in India have concentrated on education, health, welfare, protection from exploitation, juvenile justice, and shielding children from physical and psychological harm. However, the rise of digital childhood has introduced new vulnerabilities that necessitate a specialized legal approach to informational privacy, digital autonomy, and data governance specifically for minors. Digital engagement begins at increasingly younger ages, often before children fully understand data collection practices, algorithmic profiling, privacy implications, or digital manipulation techniques. This results in a structural imbalance between child users and data-driven digital systems designed to extract behavioral information.

Legal framework under DPDP ACT,2023

The introduction of the Digital Personal Data Protection Act, 2023 signifies a pivotal shift in India's legal landscape concerning digital privacy, informational autonomy, and the regulation of personal data processing. This is the first instance where India has implemented a comprehensive legal framework specifically aimed at overseeing the collection, storage, usage, transfer, and deletion of digital personal data through a rights-based and compliance-focused approach. The legislation arrives at a time when digital engagement is deeply integrated into governance, commerce, education, communication, healthcare, and daily social interactions. In this technology-driven context, personal data serves not just as information but as a strategic asset influencing economic markets, behavioral patterns, algorithmic governance, and individual autonomy. As a result, the legal regulation of personal data processing has become crucial to constitutional liberty, dignity, and democratic accountability. A notable aspect of the Act

[3] Saha, S., & Mukhopadhyay, S. (2024). A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023. *International Journal of Law and Social Sciences*, 84–95. https://doi.org/10.60143/ijls.v10.i1.2024.114

is its clear acknowledgment that children need enhanced legal protection in digital settings. This acknowledgment aligns with the growing global awareness that minors are particularly vulnerable in data-driven environments. Children frequently interact with educational platforms, gaming systems, streaming services, social networking sites, connected devices, smart applications, and AI-enabled technologies. Their digital activities generate substantial amounts of personal and behavioral data, often collected through systems designed to maximize engagement, profiling, and predictive analytics. Unlike adults, children generally lack the cognitive maturity to comprehend privacy structures, consent mechanisms, algorithmic manipulation, or long-term informational consequences. Their developmental vulnerability increases the risk of exploitation, surveillance, commercial targeting, behavioral engineering, and the erosion of future autonomy. Therefore, protecting children's data necessitates distinct legal measures beyond general privacy protections[4]. Under the Act, children are regarded as a special category of data principals, for whom additional compliance obligations are placed on data fiduciaries. The framework introduces requirements for verifiable parental consent before processing children's personal data, restrictions on tracking and behavioral monitoring of children, a ban on targeted advertising aimed at minors, increased obligations on entities processing children's data, and regulatory oversight mechanisms to ensure compliance. These provisions reflect the legislative intent to create a protective digital environment for minors[5]. While the statutory framework marks significant progress, it also introduces crucial doctrinal and practical issues. It explores statutory definitions, principles for processing child data, data fiduciaries' obligations, rights structures, enforcement mechanisms, and practical implementation challenges. The chapter aims to assess whether the Act establishes a robust, child-focused privacy regime capable of addressing modern digital threats.

Restrictions on Tracking, Behavioural Monitoring, and Targeted Advertising

The DPDP Act introduces a progressive measure for child protection by restricting exploitative digital commercial practices targeting minors.

The law enforces stringent limitations on:

(i) Tracking

Tracking refers to the continuous observation of user activities across different platforms, services, devices, or periods to develop behavioral profiles. Techniques for tracking include:

a) cookies;
b) device identifiers;
c) location analytics;
d) engagement metrics;
e) cross-platform behavioral mapping;
f) browsing pattern analysis.

[4] Dixit, A. (2026). DATA PROTECTION IN INDIA AFTER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL EVALUATION OF PRIVACY AND STATE POWER. *Indian Journal of Legal Review*, *6*(1), 116. https://doi.org/10.65393/ldeo6679

[55] Khan, M. N. I. (2025). CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES. *American Journal of Scholarly Research and Innovation*, *04*(01), 138–174. https://doi.org/10.63125/a4gbeb22

When applied to children, tracking generates comprehensive digital behavioral records that can predict vulnerabilities and influence decisions. The Act seeks to curtail such intrusive surveillance.

(ii) Behavioral Monitoring

This information can be used to increase engagement and improve retention[6]. For children, behavioral monitoring is particularly worrisome as it can lead to:

a) addiction-oriented design;
b) emotional manipulation;
c) psychological conditioning;
d) autonomy erosion;
e) developmental influence.

Therefore, limiting such monitoring focuses on child rights rather than solely on privacy[7].

(iii) Targeted Advertising

Targeted advertising uses personal data to deliver tailored commercial messages based on behavioral profiles[8]. Children are particularly susceptible because:

a) their persuasive literacy is not fully developed;
b) advertising may be perceived as entertainment;
c) influencer content blurs commercial lines;
d) behavioral targeting exploits vulnerabilities;
e) algorithmic systems can enhance persuasion.

The prohibition of targeted advertising toward children acts as a vital legal safeguard to prevent the commercial exploitation of their developmental immaturity. This aligns with the global trend of restricting behavioral advertising aimed at minors.

Critical Evaluation of the Act

The child data protection framework established by the DPDP Act marks a significant legislative achievement. However, from doctrinal, constitutional, and comparative viewpoints, it exhibits both notable strengths and significant limitations.

A. Strengths

(i) Acknowledgement of Child Vulnerability

[6] Harris, J. L., Fleming-Milici, F., Gearhardt, A. N., Grier, S., Montgomery, K., Romo-Palafox, M., & Tatlow-Golden, M. (2024). *Digital Food Marketing and Children's Health and Well-being* (pp. 81–90). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-69362-5_12

[7] Ju, I., Ham, C.-D., & Yel, E. (2025). Dark Patterns in Data-Consent Disclosures and Consumer Reactance to Online Behavioral Advertising. *Journal of Advertising*, *ahead-of-print*(ahead-of-print), 1–19. https://doi.org/10.1080/00913367.2025.2593666

[8] Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(48), 12714–12719. https://doi.org/10.1073/pnas.1710966114

For the first time, Indian data protection law explicitly recognizes the need for heightened protection for children in digital settings. This represents a substantial jurisprudential advancement.

(ii) Emphasis on Protection

The framework employs a precautionary approach that focuses on:

1. parental consent;
2. limiting exploitative tracking;
3. restricting behavioral monitoring;
4. banning targeted advertising.

This approach reflects a legislative focus on child welfare.

(iii) Consistency with Constitutional Privacy

The Act implements constitutional principles of dignity, autonomy, and informational protection as recognized in Justice K.S. Puttaswamy v. Union of India.

(iv) Commercial Limitations

Restrictions on profiling and targeted advertising directly address the commercial exploitation of children's behavioral vulnerabilities.

(v) Preventive Approach

The framework aims to prevent harmful data processing rather than merely compensating for harm after it occurs.

B. Limitations

(i) Broad Age Classification

Treating everyone under eighteen the same may overlook developmental differences among:

1. early childhood;
2. middle childhood;
3. adolescents nearing adulthood.

A 17-year-old digital user and a 7-year-old child do not have the same informational capacity.

(ii) Parent-Centric Approach

The framework heavily relies on parental consent, but:

1. parents may lack digital literacy;
2. consent may become routine;
3. some children may not have effective parental oversight;
4. parental consent does not eliminate exploitative platform design.

(iii) Verification Challenges

Obtaining verifiable parental consent may necessitate identity infrastructure that itself raises privacy concerns.

(iv) Adolescent Participation Rights

Excessive restrictions may hinder adolescents' access to:

1. educational forums;
2. civic participation platforms;
3. spaces for self-expression;
4. mental health resources;
5. beneficial digital communities.

(v) Enforcement Difficulties

Modern profiling technologies are often opaque, algorithmic, and inferential, making it legally and technically challenging to detect covert behavioral monitoring.

(vi) Need for Child-Centric Design Regulation

The Act limits certain outcomes but does not yet fully regulate:

1. addictive design;
2. dark patterns targeting minors;
3. manipulative recommendation systems;
4. harmful engagement-maximizing architecture.

Future reforms may require stronger design-based regulations.

Comparative Analysis: GDPR, COPPA, and the Digital Personal Data Protection Act, 2023

A comparative analysis of key legal systems highlights significant variations in regulatory philosophy, scope, child-focused protections, and enforcement strategies[9].

Art. 5 GDPR Principles relating to processing of personal data - Personal data must be handled in a manner that is lawful, fair, and transparent with respect to the individual concerned ('lawfulness, fairness, and transparency'). It should be gathered for specific, clear, and legitimate reasons and not processed further in ways that conflict with those reasons. Data should be stored in a way that allows identification of individuals only as long as necessary for the processing purposes. It may be retained longer if processed solely for archiving in the public interest, scientific or historical research, or statistical purposes, in line with Article 89(1), provided that appropriate technical and organizational measures are implemented to protect the rights and freedoms of the data subject ('storage limitation')[10]. Data must be processed securely, ensuring protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using suitable technical or organizational measures ('integrity and confidentiality'). Art. 6 Processing shall be lawful only if and to the extent that at least one of the following applies: The data subject has given consent to the processing of his or her personal data for one or more specific purposes; Processing is required to fulfill a contract involving the data subject or to take actions at the data subject's request before entering into a contract. Processing is also necessary to comply with a legal obligation that the controller is subject to. Additionally, processing is essential to safeguard the

[9] (Scott, 2020)

[10] Bakare, S., Adeniyi, A., Akpuokwe, C., & Eneh, N. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. *Computer Science & IT Research Journal*, *5*(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859

vital interests of the data subject or another individual. It is also required for performing a task in the public interest or exercising official authority granted to the controller. The Union or Member State law must meet a public interest objective and be proportionate to the legitimate aim pursued[11].

A. Regulatory Philosophy

The GDPR embraces a comprehensive rights-based framework rooted in dignity, informational self-determination, and human rights principles. It views children as vulnerable individuals with rights, warranting additional protections.

In contrast, COPPA primarily focuses on parental control over the collection of children's data, with a narrower and more commercially driven scope.

India's DPDP Act takes a middle ground, incorporating robust protective measures akin to European child-safety concerns while heavily relying on parental consent mechanisms similar to COPPA.

B. Age Thresholds

Framework Child Age Threshold-

a. GDPR: 13–16 years (member state discretion)
b. COPPA; Below 13 years
c. DPDP Act: Below 18 years

India employs the broadest definition, reflecting a highly protective stance. However, critics argue that the strict eighteen-year threshold may not adequately acknowledge adolescent autonomy and evolving capacities.

C. Parental Consent

All three frameworks involve parental participation, but the degree varies.

COPPA heavily relies on verifiable parental consent as its primary regulatory tool.

GDPR uses parental consent more selectively, embedding broader rights protections.

The DPDP Act also requires verifiable parental consent but adds further restrictions on behavioral monitoring and targeted advertising.

Thus, India's framework offers more substantive protection than COPPA.

D. Behavioral Profiling and Advertising

The GDPR imposes strict regulations on profiling and automated decision-making, with European regulators increasingly discouraging behavioral advertising aimed at children.

COPPA has historically concentrated more on data collection than on sophisticated profiling systems.

The DPDP Act explicitly limits:

[11] Macenaite, M., & Kosta, E. (2017). Consent for processing children's personal data in the EU: following in US footsteps? *Information & Communications Technology Law*, *26*(2), 146–197. https://doi.org/10.1080/13600834.2017.1321096

I. tracking;

II. behavioral monitoring;

III. targeted advertising directed at children.

IV. This is one of the stronger child-protective features of Indian legislation.

E. Child-Centered Transparency

The GDPR places a strong emphasis on clear and understandable communication for children.

India's framework currently lacks detailed statutory standards regarding child-friendly notices, age-appropriate transparency design, and simplified explanation architecture.

Future regulatory developments may need to address this gap.

F. Enforcement Structure

The GDPR boasts the most robust enforcement architecture through :

a. independent supervisory authorities;

b. substantial administrative penalties;

c. detailed compliance obligations.

d. COPPA enforcement relies heavily on the Federal Trade Commission.

India's enforcement framework is still developing, and its long-term effectiveness will depend on:

a. regulatory independence;

b. technical expertise;

c. institutional capacity;

d. enforcement consistency.

Global Best Practices in Child Data Protection

Comparative studies highlight several emerging global best practices pertinent to the governance of child privacy

i. Privacy by Design Platforms should integrate privacy protection during the design phase, rather than considering compliance as an afterthought.

ii. Safety by Default Child accounts should automatically be set to the highest privacy settings.

iii. Age-Appropriate Design Digital services should tailor interfaces, transparency features, and risk structures to suit developmental maturity.[12]

iv. Data Minimization Only essential information should be collected from children

[12] D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., Montjoye, Y.-A., & Bourka, A. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. In *arXiv (Cornell University)*. Technische Universitat Dresden. https://doi.org/10.48550/arxiv.1512.06000

v. Restriction on Profiling The commercial behavioral profiling of children should be minimized or banned.

vi. Child-Friendly Transparency Privacy information should be accessible to minors, avoiding complex legal jargon.

vii. Strong Enforcement. Effective sanctions are crucial to ensure compliance by major digital companies.[13]

viii. Algorithmic Accountability Platforms should assess and address developmental harms caused by recommendation systems and predictive analytics. These best practices are increasingly shaping global expectations for ethical digital governance concerning minors.

Lessons for India

A comparative analysis provides several key insights for enhancing India's framework for protecting children's data.

A. Necessity for Age-Specific Regulation

India might explore more refined strategies that acknowledge the different maturity levels of adolescents instead of treating everyone under eighteen the same way.

B. Child-Friendly Transparency Standards

The legal framework should mandate simplified, age-appropriate explanations that are easy for children and their guardians to understand.

C. Design-Focused Regulation

Future reforms should tackle issues such as:

1) addictive interface designs;

2) manipulative engagement systems;

3) dark patterns aimed at minors;

4) emotionally exploitative recommendation systems.

D. Enhanced Regulatory Guidance

There is a need for detailed operational rules concerning:

1) parental verification;

2) profiling limitations;

3) compliance with educational technology;

4) platform accountability;

5) clear instructions

[13] Berson, I. R., Berson, M. J., & Luo, W. (2025). Innovating responsibly: ethical considerations for AI in early childhood education. *AI, Brain and Child*, *1*(1). https://doi.org/10.1007/s44436-025-00003-5

E. Independent Oversight

Strong enforcement institutions with technical expertise are crucial.

F. Rights-Based Child Governance

India can advance beyond a solely consent-focused protection model towards a broader child-rights-oriented digital governance that balances:

1) protection;

2) participation;

3) developmental autonomy.

Challenges in Age Verification

One of the primary challenges in implementing the Digital Personal Data Protection Act, 2023, revolves around age verification. Since protections for children apply to those under eighteen, platforms need a way to ascertain if a user is a minor. However, ensuring accurate age verification in digital spaces is fraught with technical, legal, and ethical complexities.

Currently, most digital services depend on users self-reporting their age by entering a birth date when setting up accounts. These systems are easily bypassed and offer minimal protection. Children often falsify their age to gain access to social media, gaming platforms, communication apps, or age-restricted content. As a result, formal compliance measures may prove ineffective in practice.

A. Privacy Paradox in Age Verification

A significant issue is that more robust age verification systems might necessitate collecting additional personal data, thus increasing privacy invasion. To verify age accurately, platforms might require:

- government-issued IDs;
- biometric data;
- facial recognition analysis;
- parental identification records;
- third-party authentication information.

This creates a paradox: safeguarding child privacy might demand more extensive data collection.

Excessive identity verification systems could expose children and families to surveillance risks, data breaches, identity theft, unauthorized retention of sensitive information.

Therefore, age verification mechanisms must adhere to principles of proportionality, necessity, and data minimization.

B. Technological Limitations

- Current age estimation technologies are flawed and may result in:
- false positives;
- discriminatory outcomes;

- inaccurate classifications;
- exclusionary errors.

AI-based facial age estimation systems, for example, might yield biased results based on ethnicity, lighting, disability, or image quality. Such inaccuracies could wrongly deny access to legitimate users or fail to adequately protect minors.

C. Access and Inclusion Concerns

Strict verification requirements might disproportionately impact:

economically disadvantaged users;

- rural populations without formal documentation;
- children sharing devices with family members;
- users with limited digital literacy.

Thus, overly burdensome verification systems could lead to digital exclusion.

D. Regulatory Uncertainty

The DPDP framework currently leaves many operational details about age verification to subordinate regulation and implementation guidance. The lack of detailed standards could lead to inconsistent industry practices and uncertainty about acceptable verification mechanisms.

Therefore, age verification remains one of the most challenging unresolved issues in child data governance.

Enforcement and Regulatory Challenges

Even the most robust legal framework is rendered ineffective without reliable enforcement mechanisms. Safeguarding children's personal data encounters significant enforcement challenges due to the technological complexity, rapid evolution, and often transnational nature of digital ecosystems.

A. Cross-Border Data Processing

Numerous digital platforms in India are multinational corporations that handle data through globally dispersed infrastructures. Personal data might be:

i. stored in various jurisdictions;
ii. processed via foreign cloud systems;
iii. analyzed using international AI infrastructure.

This situation complicates: jurisdictional oversight, investigative authority, enforcement of domestic orders, and cross-border accountability.

B. Technological Opacity

Contemporary algorithmic systems are notably opaque. Platforms might utilize:

i. machine learning systems;
ii. automated recommendation engines;
iii. predictive behavioral analytics;

iv. inferential data modeling.

Regulators may find it challenging to ascertain: what information is collected, how profiling is conducted, whether behavioral monitoring is occurring indirectly, how recommendation systems impact children.

As a result, enforcement increasingly demands advanced technical expertise.[14]

C. Institutional Capacity

Effective enforcement necessitates:

i. trained regulatory personnel;

ii. technological infrastructure;

iii. cybersecurity expertise;

iv. investigative capability;

v. digital forensic competence.

Building such institutional capacity poses a significant challenge for emerging regulatory systems.

D. Compliance Burden and Industry Resistance

Digital companies might resist stringent regulations where compliance impacts:

i. advertising revenue;
ii. behavioral analytics systems;
iii. data monetization strategies;
iv. engagement optimization models.

Thus, strong enforcement may face economic and political resistance from powerful technology sectors.

E. Detection Difficulties

Violations involving covert profiling or hidden tracking can be difficult to detect because users and parents often cannot observe invisible data processing practices. Harm may occur silently over extended periods without immediate visible consequences.

Therefore, enforcing child privacy laws requires a proactive regulatory framework rather than relying solely on complaint-based systems.[15]

[14] Walker, K. L., Bodendorf, K., Kiesler, T., De Mattos, G., Rostom, M., & Elkordy, A. (2023). Compulsory technology adoption and adaptation in education: A looming student privacy problem. *Journal of Consumer Affairs*, *57*(1), 445–478. https://doi.org/10.1111/joca.12506

[15] Imohimi, E. O. (2025). Building Privacy and Preserving AI Models for Secure Student Data Management in Educational Technology Platforms. *Journal of Intelligent Learning Systems and Applications*, *17*(03), 149–171. https://doi.org/10.4236/jilsa.2025.173011

Balancing Protection with Participation Rights

One of the most intricate normative challenges in child privacy law involves finding a balance between protective regulations and children's rights to engage in digital activities, communicate, learn, and express themselves. Children are increasingly reliant on digital platforms for various purposes, including:

- educational opportunities;
- social interactions;
- creative outlets;
- mental health support;
- civic involvement;
- development of professional skills.

Thus, overly stringent restrictions might inadvertently curtail valuable opportunities.

A. Risks of Protection-Focused Regulation

Highly restrictive laws could lead to:

i. exclusion from online communities;
ii. obstacles to accessing educational materials;
iii. limited access to information;
iv. excessive reliance on parental consent;
v. hindrance of adolescent independence.

Children should not be viewed merely as passive entities needing protection; they are evolving individuals with rights to participate and exercise agency.

B. Principle of Evolving Capacity

International child rights law acknowledges that autonomy develops over time. Adolescents often have a greater ability to:

i. comprehends digital landscapes;

ii. make informed choices;

iii. evaluate online risks;

iv. exercise control over their information.

Therefore, legal systems should avoid treating all minors uniformly.

C. Necessity for Balanced Governance

Effective governance of child privacy should aim to:

i. protect against exploitation;
ii. uphold dignity;
iii. support developmental independence;
iv. ensure safe digital engagement;
v. empower through digital literacy.

This calls for nuanced regulation rather than purely paternalistic restrictions.

D. Digital Literacy as a Structural Safeguard

Long-term protection of child privacy cannot rely solely on legal prohibitions. Sustainable governance also necessitates: education in digital literacy;

i. awareness of online risks;
ii. child-friendly privacy education;
iii. fostering a responsible platform culture;
iv. parental awareness programs.

Thus, empowerment and education complement legal regulations.

RECOMMENDATIONS

Recommendation 1: Implement an Age-Specific Regulatory Framework

India should contemplate establishing more detailed age classifications that acknowledge the developmental distinctions among:

a) younger children;

b) middle adolescents;

c) older teenagers.

d) A tiered strategy would more effectively balance: protection, autonomy, participation rights, evolving capacities.

One of the primary drawbacks of the Digital Personal Data Protection Act, 2023 is its blanket definition of a "child" as anyone under the age of eighteen. Although this reflects a strong intent to protect, it does not sufficiently account for the developmental, psychological, and cognitive variations among children of different ages. A thirteen-year-old and a seventeen-year-old have significantly different levels of maturity, digital literacy, decision-making skills, and awareness of online dangers. Treating all minors the same could therefore lead to both practical and legal challenges. Implementing an age-specific or tiered regulatory framework would enable the law to offer tailored protections based on the evolving capacities and maturity levels of children. This approach is increasingly acknowledged internationally as a more balanced and effective way to regulate children's digital engagement and informational privacy.

A. Necessity for an Age-Specific Framework

Children's interactions with digital platforms vary based on their age, educational background, emotional growth, and social surroundings. Younger children often struggle to comprehend:

- privacy policies;
- behavioral tracking;
- targeted marketing;
- data sharing risks;
- online manipulation.

In contrast, older adolescents may have a higher level of digital literacy and actively use digital platforms for: learning, skill enhancement, professional networking, social engagement, creative pursuits, civic involvement.

Thus, a strict regulatory framework that applies the same restrictions to everyone under eighteen could hinder adolescent autonomy and participation rights while imposing unnecessary compliance challenges on digital platforms. The principle of evolving capacities, acknowledged in international child rights law, recognizes that children gradually gain the ability to make informed choices as they grow. Therefore, digital regulation should adapt according to age and developmental understanding.

B. Suggested Tiered Classification

India might consider implementing a three-tier age classification system for digital privacy governance.

1. Younger Children (Under 13 Years)

Children under thirteen typically have limited understanding of:

a. online surveillance practices;

b. data monetization systems;

c. algorithmic recommendations;

d. commercial manipulation.

Therefore, this age group should receive the highest level of legal protection.

Proposed Safeguards: mandatory parental consent, strict prohibition on behavioral profiling, complete ban on targeted advertising, highly restricted data collection, child-safe default privacy settings, prohibition on manipulative interface design.

This model resembles the approach taken under the United States COPPA framework, which specifically applies to children under thirteen.

2. Middle Adolescents (13–16 Years)

Children in this age group often start using digital platforms independently for educational and social purposes. They may have a partial understanding of digital systems, but remain vulnerable to:

a. peer pressure;

b. addictive platform design;

c. emotional manipulation;

d. profiling systems.

e. For this group, regulation should balance protection with guided autonomy.

Proposed Safeguards: simplified and age-appropriate privacy notices, shared consent mechanisms involving both parents and adolescents, restrictions on behavioral advertising, transparency regarding algorithmic recommendations, enhanced educational privacy safeguards.

This approach incorporates elements of the European Union GDPR framework, where member states may lower the age of digital consent to thirteen while still requiring safeguards for minors.

3. Older Teenagers (16–18 Years)

Older adolescents generally exhibit greater maturity and digital awareness. Many in this category actively participate in:

a. online education;

b. internships;

c. e-commerce;

d. professional communication;

e. content creation;

f. digital financial systems.

Excessive parental control in this age group may interfere with: informational autonomy, privacy rights, freedom of expression, and independent participation in digital society.

Therefore, regulation for this group should focus on informed participation rather than absolute restriction.

Proposed Safeguards: independent consent rights subject to limited safeguards, stronger transparency obligations, right to access and erase data, restrictions on exploitative profiling, protection from manipulative algorithms, such an approach would better respect adolescent dignity and evolving autonomy.[16]

C. Global Strategies for Age-Specific Regulation

1. European Union – GDPR

The GDPR in the European Union acknowledges the need for special protection for children while allowing flexibility in setting the age for digital consent. Article 8 generally requires parental consent for those under sixteen, but member states can lower this to thirteen. This adaptable framework acknowledges that: maturity develops over time, different age groups have varying abilities, digital engagement should not be overly restricted.

Several European nations have implemented varied approaches:

- Ireland: age limit of 16;
- France: 15 years;
- Germany: 16 years in many situations;
- Spain: 14 years.

The GDPR also stresses the importance of transparency that is child-friendly and communication that is suitable for different ages.

2. United States – COPPA

COPPA specifically targets children under thirteen, requiring verifiable parental consent before collecting personal data. Although the age limit is relatively low, it highlights the need for increased protection for younger children due to their limited understanding of digital risks. Critics, however, argue that the

[16] Shouli, A., Barthwal, A., Campbell, M., & Shrestha, A. (2025). Ethical AI for Young Digital Citizens: A Call to Action on Privacy Governance. In *arXiv (Cornell University)*. Technische Universitat Dresden. https://doi.org/10.48550/arxiv.2503.11947

framework does not adequately address teenagers aged thirteen to eighteen, who also face issues like behavioral profiling and algorithmic influence[17].

3. United Kingdom – Age-Appropriate Design Code

The UK has implemented the Age-Appropriate Design Code within its data protection framework to ensure digital services cater to children's developmental needs. The Code uses a risk-based and age-sensitive approach, focusing on:

- default high privacy settings;
- minimal data collection;
- banning nudging techniques;
- transparency that suits different age groups.

This is considered one of the most advanced child-focused digital governance models globally[18].

4. Australia

Australia has increasingly focused on online safety regulation through child-centric digital safety standards and stricter requirements for digital platforms. Discussions in Australia also support age-sensitive approaches to online engagement and child privacy.

D. Benefits of an Age-Specific Regulatory Framework

1. Enhanced Protection for Younger Children

Younger children would receive stronger protection against: surveillance, exploitation, manipulative advertising, and addictive interface designs.

2. Acknowledgment of Adolescent Independence

Older teenagers would gain greater respect for, informational privacy, independent participation, freedom of expression, digital autonomy.

3. Enhanced Regulatory Precision

Different obligations could be tailored based on: level of vulnerability, type of digital activity, risks associated with processing. This would lead to more balanced and proportionate regulation.

4. Improved Compliance Mechanisms

Digital platforms could implement: age-appropriate privacy settings, differentiated transparency tools, customized safety measures. This would enhance practical enforceability.

E. Challenges in Implementing an Age-Specific Model

[17] Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., & Egelman, S. (2018). "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies*, *2018*(3), 63–83. https://doi.org/10.1515/popets-2018-0021

[18] Bygrave, L. A. (2017). Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements. *Oslo Law Review*, *4*(2), 105–120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

While this framework offers advantages, its implementation is not without challenges.

1. Difficulties in Verifying Age- Accurately determining age without resorting to excessive monitoring is challenging.

2. Risk of Excessive Data Collection- Age verification systems might necessitate intrusive gathering of identity information.

3. Technological Complexity- Platforms could encounter compliance issues when creating multiple age-specific systems.

4. Socio-Economic Barriers- Children from economically disadvantaged backgrounds might lack access to identity verification tools or digital literacy support.

F. Need for a Balanced Indian Approach

India's digital landscape is highly diverse in terms of: literacy levels, technological access, parental supervision, socio-economic conditions.

Thus, India should implement a balanced framework that:

- rigorously protects younger children;
- gradually increases adolescent autonomy;
- promotes digital literacy;
- encourages privacy-by-design obligations;
- ensures accountability of digital intermediaries.

An age-specific regulatory model would better align with constitutional principles of dignity,

Recommendation 2: Establish Child-Friendly Transparency Standards

Privacy notices intended for children should be: clear; visual; age-appropriate; simple to comprehend; and available in easy-to-access formats. Complex legal documents should not substitute for true transparency.

Recommendation 3: Strengthen Regulation of Algorithmic Systems

Future reforms should specifically target: addictive interface designs; dark patterns aimed at minors; manipulative recommendation systems; emotional analytics; behavioral engineering frameworks. Platforms that manage children's data should be required to conduct mandatory algorithmic risk assessments.

Recommendation 4: Establish Stronger Educational Data Governance

Educational technology systems should comply with specialized regulations that mandate: strict limitations on purpose; prohibition of student data commercialization; reduction of behavioral analytics; restricted data retention durations; improved cybersecurity standards. Access to education should not depend on excessive data extraction. [19]

[19] Berson, I. R., Berson, M. J., & Luo, W. (2025). Innovating responsibly: ethical considerations for AI in early childhood education. *AI, Brain and Child*, *1*(1). https://doi.org/10.1007/s44436-025-00003-5

Recommendation 5: Strengthen Regulatory and Enforcement Capacity

Effective implementation requires: technologically proficient regulatory staff; digital forensic skills; algorithmic auditing capabilities; independent oversight bodies; proactive compliance monitoring. Without strong enforcement, statutory protections may remain merely symbolic.

Recommendation 6: Promote Digital Literacy and Awareness

The Government, educational institutions, and civil society should develop: child-centered digital literacy programs; parental awareness initiatives; school-based privacy education; public campaigns on online safety and behavioral manipulation. Empowerment through education is essential for long-term protection.

Recommendation 7: Encourage Privacy by Design and Safety

Design Digital platforms should incorporate child protection measures from the initial design stage by: setting default privacy settings to high; collecting minimal data; restricting behavioral tracking; creating a child-friendly interface architecture. Compliance should be integrated structurally rather than just procedurally.[20]

CONCLUSION

In today's digital age, children are consistently engaged in complex data-driven settings where their personal data functions as identity, a behavioral resource, an economic asset, and a means of influence. While digital technologies provide significant educational, social, and developmental advantages, they also expose children to new types of surveillance, profiling, commercialization, and algorithmic manipulation.

Consequently, protecting children's personal data is essential to preserving their dignity, autonomy, developmental freedom, and democratic participation in modern society. This dissertation has demonstrated that the Digital Personal Data Protection Act, 2023 represents a crucial and necessary advancement in Indian privacy law. By recognizing children as a specially protected group and curbing exploitative digital practices, the legislation establishes an important legal foundation for child-focused data governance.

However, the research also reveals that effective child privacy protection extends beyond formal consent mechanisms and statutory declarations. Contemporary privacy harms increasingly arise from invisible behavioral surveillance, algorithmic influence, predictive analytics, manipulative engagement systems, and the commercialization of developmental vulnerabilities.

Therefore, future child privacy governance in India must evolve towards rights-based digital regulation, enhanced accountability mechanisms, child-centered technological design, a balanced acknowledgment of autonomy and protection, robust institutional enforcement, and widespread digital literacy. Ultimately, safeguarding children's personal data is not merely a technological or regulatory issue it is a constitutional, ethical, and societal responsibility.

[20] Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive*, *14*(1), 1146–1163. https://doi.org/10.30574/ijsra.2025.14.1.0225

The manner in which legal systems regulate children's digital environments will affect not only privacy outcomes but also the future of autonomy, childhood, citizenship, and human dignity in the digital era.

SUGGESTIONS & STRATEGIC RECOMMENDATIONS

The dissertation details explicit operational and systemic recommendations to transition India's data governance framework from a reactive model to a preventive model:

I. Adopt a Layered, Age-Appropriate Regulatory Framework: India should move away from the uniform 18-year age definition for children and take inspiration from the GDPR, COPPA, or the UK Age-Appropriate Design Code (AADC). This would entail a tiered system that offers stringent protection for younger age groups while enhancing the autonomy and informational self-determination of teenagers.

II. Require Child-Friendly Transparency Measures: Technology platforms need to replace lengthy, complex, and jargon-laden privacy policies with simplified, visually engaging, multilingual, and age-appropriate notifications that are easily comprehensible for both children and their guardians.

III. Control Platform Design and Algorithmic Weaknesses: Future legislative efforts should limit systemic "dark patterns," addictive design loops, engagement-focused architectures, and emotional analytics aimed at minors. Platforms should be legally obligated to conduct mandatory algorithmic risk evaluations.

IV. Implement Specialized Educational Data Governance: The EdTech sector needs stricter rules on purpose limitation. Access to digital learning platforms should never be legally or practically dependent on excessive data collection, behavioral analytics, or the commercialization of a student's educational journey.

V. Enhance Institutional and Technological Capabilities: The Data Protection Board (DPB) or equivalent oversight entities must be equipped with technical auditing resources to detect backend, inferred data profiling rather than just reviewing legal documentation.