



Children's Online Privacy and Constitutional Protection: An Indian Legal Perspective in the Age of Data-Driven Platforms

Dr. Surendra Kumar

Principal, Mahavir Law College Kiran Path, Mansarovar, Jaipur

Abstract

Digital technologies have become integral to children's education, recreation, communication and access to information. During ordinary online activity, however, applications, educational platforms, games, connected devices and social-media services may collect children's names, images, location, browsing behaviour, contact information, biometrics and inferred interests. Such data may be used for profiling, targeted advertising, recommendation systems and automated decision-making. Children are especially vulnerable because they may not understand the future consequences of disclosure, possess limited bargaining power and remain dependent upon adults and institutions for protection.

This article examines children's online privacy as a constitutional and child-rights issue, with particular reference to India. It adopts a qualitative and doctrinal methodology based on the Constitution of India, Supreme Court privacy jurisprudence, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Information Technology Act and Rules, the Protection of Children from Sexual Offences Act and international child-rights standards. The study finds that the Indian constitutional framework can protect children's dignity, autonomy, equality, development and informational privacy through Articles 14, 19 and 21, read with Article 21A and the Directive Principles concerning child welfare.

The Digital Personal Data Protection Act creates important child-specific obligations, including verifiable parental consent and prohibitions on harmful processing, behavioural monitoring and targeted advertising. As of August 2026, however, these substantive provisions had not yet commenced; they are scheduled to become effective eighteen months after the Gazette notification of 13 November 2025. The article argues that parental consent alone cannot secure children's privacy. India requires age-appropriate design, data minimisation, child-accessible notices,



stronger safeguards for educational technology, independent audits, proportionate age assurance and remedies that recognise children's evolving capacities.

Keywords: Children's privacy, constitutional protection, personal data, online platforms, parental consent, digital rights, age-appropriate design.

1. Introduction

The internet is no longer a separate space that children occasionally enter. Educational lessons, examinations, entertainment, friendships, games, healthcare information and creative participation increasingly occur through digital systems. Globally, 82 per cent of people aged 15–24 used the internet in 2025, indicating the central place of digital communication in young people's lives. Access nevertheless remains unequal across income groups, regions and households.

Digital participation can strengthen children's rights to education, information, expression, association and play. At the same time, every online interaction may generate data. A learning application may record performance, attention, device information and time spent on each question. A game may collect location, contacts, voice recordings and behavioural patterns. Social-media services can analyse viewing habits, relationships and emotional responses. Connected toys and wearable devices may continuously collect information from a child's home and body.

Privacy in this environment cannot be reduced to secrecy. It includes the child's ability to develop a personality without constant surveillance, to communicate confidentially, to make age-appropriate choices and to prevent permanent judgments based upon childhood behaviour. A child may disclose information without understanding that it can be copied, combined with other records or used years later for commercial and institutional decisions.

The problem is intensified by the unequal relationship between children and digital companies. Privacy policies are often long and technical, while refusal of data collection may mean exclusion from a service required for education or social participation. Children cannot meaningfully negotiate such conditions. Parents may also lack technical knowledge and may themselves disclose extensive information about children through photographs, school details and location-tagged posts.

Constitutional protection is therefore necessary not merely after a data breach but at the stage of system design. The central legal question is whether children must carry the burden of protecting themselves, or whether platforms, schools and the State must create environments in which privacy is protected by default.

2. Meaning and Dimensions of Children's Online Privacy

Children's online privacy includes control over personal data, communications, reputation, bodily information, domestic life and identity. The Convention on the Rights of the Child provides that no child shall be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, or to unlawful attacks upon honour and reputation.



The United Nations Committee on the Rights of the Child has clarified that children remain full rights-holders in digital environments. Protection should be guided by non-discrimination, the best interests of the child, survival and development, and respect for children's views. Digital access can advance numerous rights, but commercial practices, surveillance and unsafe design may also interfere with them.

Online privacy has several interconnected dimensions:

Informational privacy concerns the collection, processing, disclosure, retention and deletion of data. Personal data include direct identifiers, such as a name or photograph, and indirect information from which a child can be identified.

Communicational privacy protects messages, searches, calls and interactions from unjustified access by companies, authorities, strangers or family members.

Bodily privacy concerns photographs, videos, health information, biometric identifiers, voice samples and data generated by wearable devices.

Decisional privacy protects the space required for children to develop opinions, interests and relationships without constant manipulation or monitoring.

Reputational privacy concerns the digital record created by the child, parents, schools and other users. Childhood errors or embarrassing material can remain searchable long after the child has matured.

Privacy should be balanced with protection from abuse. Parents and schools may legitimately supervise younger children, while platforms may process information to prevent sexual exploitation or restrict access to harmful content. Yet surveillance presented as protection can itself become excessive. The appropriate standard is necessity, proportionality and respect for the child's evolving capacities rather than unrestricted adult control.

3. Major Threats to Children's Online Privacy

3.1 Commercial profiling and behavioural advertising

Many digital services depend upon continuous observation of users. Search history, viewing time, purchases, location and interaction patterns may be combined to infer preferences and vulnerabilities. A child may therefore be profiled even without directly providing sensitive information.

Profiling can influence which advertisements, videos, games or news items appear. It may exploit impulsiveness, social comparison and fear of exclusion. When recommendation systems repeatedly respond to a child's behaviour, they may shape interests rather than merely identify them. Commercial surveillance is especially problematic because children cannot fully appreciate the cumulative consequences of persistent data collection.

3.2 Educational technology and institutional surveillance

Schools increasingly use learning-management systems, attendance applications, online assessment, facial recognition, proctoring software and classroom analytics. Such tools may



improve administration or personalised learning, but they can also collect large quantities of sensitive information.

UNICEF has observed that some educational technologies track student location and online activity and share or commercially exploit information without clear consent or oversight. Its recent guidance recommends that online safety and data governance be integrated into educational planning and that EdTech tools be rigorously evaluated before large-scale adoption. A child cannot freely refuse a platform selected by the school. Parental consent is also questionable when refusal would interrupt education. Schools must therefore demonstrate that collection is educationally necessary, proportionate and free from unrelated commercial use.

3.3 Age verification and identity collection

Age assurance can protect children from adult content and help services apply appropriate safeguards. Yet highly intrusive age verification may require identity documents, facial analysis or biometric information. A mechanism intended to reduce risk may create an additional database vulnerable to breach or misuse.

Age assurance should therefore disclose as little information as possible. In many situations, a service needs to know only whether a user is above or below a particular threshold, not the person's full identity or date of birth.

3.4 Sharenting and adult disclosure

Parents commonly share photographs, school achievements, medical experiences and family details online. Such disclosure may be affectionate and well intentioned, yet it creates a digital identity before the child can participate in the decision.

Children's dignity requires adults to consider whether publication may expose the child to embarrassment, profiling, identity misuse or unwanted recognition. Parental responsibility is not parental ownership of the child's identity. As children mature, their views regarding continued publication and deletion should receive increasing weight.

3.5 Data breaches and identity misuse

Children's records may remain useful to criminals for long periods because children are less likely to monitor financial or identity activity. A breach involving school records, health information, passwords or biometric identifiers can create consequences extending into adulthood.

Unlike a password, biometric information cannot easily be replaced. Collection of facial, fingerprint or voice data from children should therefore be permitted only when strictly necessary and protected through stronger security and retention limits.

3.6 Sexual exploitation and fabricated content

Online privacy violations may overlap with sexual abuse. The POCSO Act treats repeated electronic contact, threats involving real or fabricated depictions of a child and the use of children in digital pornographic material as offences. Its definition of child pornography includes computer-generated or modified images that appear to depict a child.



Artificial intelligence increases the possibility of creating realistic sexualised images from ordinary photographs. Privacy protection must therefore cover both authentic data and fabricated content that falsely attaches sexual conduct to an identifiable child.

4. Objectives and Methodology

The study seeks to examine the constitutional basis of children's online privacy; analyse India's current statutory framework; identify gaps in parental-consent and platform-governance models; and recommend child-centred reforms.

A qualitative and doctrinal method has been used. Primary sources include constitutional provisions, Supreme Court decisions, central legislation, statutory rules and Gazette notifications. International and comparative materials have been drawn from the United Nations, UNICEF, the European Union, the United Kingdom and the United States. No primary survey or experimental data have been created.

5. Constitutional Basis of Children's Online Privacy

5.1 Privacy, dignity and liberty under Article 21

In *Justice K. S. Puttaswamy (Retd.) v. Union of India*, a nine-judge Bench of the Supreme Court recognised privacy as a constitutionally protected right intrinsic to life and personal liberty under Article 21 and connected with the freedoms guaranteed by Part III. The judgment linked privacy with dignity, autonomy, identity and the ability to make personal choices.

Children are rights-bearing individuals; they do not receive constitutional dignity only upon adulthood. Constant commercial observation may influence their choices, while permanent data records may limit future opportunities. Informational privacy is therefore connected with the child's freedom to learn, experiment and mature without every action becoming a permanent institutional judgment.

Privacy is not absolute. The State may interfere where there is lawful authority, a legitimate aim and a proportionate relationship between the measure and its objective. Child-safety monitoring may therefore be lawful, but indiscriminate collection or indefinite retention cannot be justified merely by using the language of safety.

5.2 Equality and non-discrimination

Articles 14 and 15 require equality and permit special provisions for children. Digital systems may reproduce discrimination when algorithms rely upon language, location, disability, caste-associated information, economic status or historical educational performance.

A child from a disadvantaged household may be profiled as less likely to succeed or pay for services. Limited digital access may itself be treated as lack of ability. Constitutional equality therefore requires examination of both direct discrimination and apparently neutral technologies that have unequal effects.

5.3 Freedom of expression and access to information

Article 19(1)(a) protects freedom of speech and expression. Children's privacy and expression should not be treated as competing absolutes. Anonymous exploration, private communication



and freedom from surveillance can make expression possible, especially for adolescents seeking information about health, identity or family problems.

Overbroad parental monitoring may discourage children from accessing legitimate information. UNICEF consequently treats privacy, freedom of expression, access to diverse information and protection of reputation as mutually connected rights that should be respected according to children's evolving capacities.

5.4 Education, development and the best interests of the child

Article 21A guarantees free and compulsory education for children between six and fourteen years. Digital education must therefore be accessible, but access cannot be made conditional upon unnecessary surrender of privacy.

Articles 39(e) and 39(f) direct the State to protect children from abuse and ensure their development in conditions of freedom and dignity. These principles support a positive constitutional obligation to regulate harmful platform design and protect children's data rather than merely punish misuse after it occurs. The current official text of the Constitution incorporates these fundamental rights and child-protection directives.

6. Indian Statutory Framework

6.1 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act defines a child as an individual below eighteen years. Section 9 requires a Data Fiduciary to obtain verifiable parental consent before processing a child's personal data. It prohibits processing likely to cause a detrimental effect on the child's well-being and prohibits tracking, behavioural monitoring and targeted advertising directed at children. Contravention of the additional child-related obligations may attract a monetary penalty extending to ₹200 crore.

These protections are significant because they shift responsibility from the child to the organisation determining the purposes and means of data processing. The ban on behavioural monitoring and targeted advertising directly addresses commercial surveillance.

The Act also permits prescribed exemptions and allows the Central Government to exempt processing above a notified age where a Data Fiduciary has demonstrated verifiably safe processing. This creates flexibility but also requires transparent standards to prevent inconsistent protection.

A crucial limitation concerns commencement. On 13 November 2025, the Central Government notified a phased implementation schedule. Sections 3–17, including the substantive obligations under section 9, are to come into force eighteen months after the notification. Consequently, as of 2 August 2026, section 9 had not yet become operational; it is scheduled to commence in May 2027.

6.2 Digital Personal Data Protection Rules, 2025

The final Rules were notified on 13 November 2025. Rule 10 provides that a Data Fiduciary must use appropriate technical and organisational measures to obtain verifiable parental consent and



check that the person identifying as the parent is an identifiable adult. Verification may use reliable identity and age details or a virtual token issued through an authorised entity, including a Digital Locker service provider.

Rules 10 and 12 are also subject to the eighteen-month commencement period and were not yet effective in August 2026.

The Rules create exemptions for healthcare, education, childcare and transportation. Educational institutions may undertake tracking or behavioural monitoring for educational activities or the safety of enrolled children. Real-time location tracking may also be undertaken for safety and protection.

These exemptions respond to legitimate needs but require strict interpretation. “Educational activities” could otherwise become an open-ended basis for monitoring attention, emotion, browsing and behaviour. Schools should be required to document necessity, prohibit commercial reuse and periodically erase information.

6.3 Information Technology Act and the 2011 Rules

Until the core DPDP provisions commence, data protection remains partly dependent upon the Information Technology Act and the Sensitive Personal Data Rules, 2011. Section 43A addresses negligence by a body corporate in maintaining reasonable security practices for sensitive personal data. The framework is not child-specific and is limited in scope, particularly when compared with the comprehensive obligations envisaged by the DPDP Act.

The Information Technology Act also penalises certain privacy violations, identity theft and publication of sexually explicit content. These provisions address misuse and criminal conduct but do not create a complete system governing routine profiling, recommendation algorithms or children’s commercial data.

6.4 Intermediary Guidelines

The Information Technology Rules require intermediaries to make reasonable efforts to prevent users from hosting information that invades another person’s privacy or is harmful to a child. They also require grievance mechanisms and classify a child as a person below eighteen. Online curated-content services must use age verification and access controls for adult-rated content.

The February 2026 amendments introduced additional obligations concerning synthetically generated content, including child sexual exploitation material and privacy-invasive synthetic imagery. These rules mainly govern content and intermediary conduct; they do not replace a comprehensive data-protection regime.

6.5 POCSO and confidentiality laws

The POCSO Act protects children from electronic sexual harassment, fabricated sexual depictions and pornographic exploitation. It contains mandatory reporting duties and child-sensitive procedures. The Act expressly recognises the child’s privacy and confidentiality throughout the judicial process.



The Juvenile Justice Act separately protects the confidentiality and identity of children involved in child-protection and justice proceedings.

These laws provide strong protection in abuse cases, but they do not address every form of data extraction, commercial profiling or school surveillance.

7. Gaps in the Existing Framework

The first difficulty is the temporary implementation gap. Parliament enacted child-specific data protections in 2023, but the central obligations will not operate until May 2027. During this period, children's routine commercial data practices remain governed by a fragmented and comparatively limited framework.

Second, the DPDP model relies heavily upon parental consent. Parents play an essential protective role, but consent may be uninformed, mechanically obtained or impossible where a child lacks a safe relationship with the parent. Adolescents may also need confidential access to counselling, health information or support services.

Third, the Act treats all persons below eighteen as one category. A six-year-old and a seventeen-year-old possess different levels of understanding and autonomy. A child-rights framework should progressively recognise the child's views and evolving capacities rather than rely exclusively upon adult authorisation.

Fourth, verifying parental consent may itself increase data collection. If platforms gather identity documents from both parent and child, the privacy mechanism may generate an additional risk. Token-based and privacy-preserving age assurance should be preferred.

Fifth, "detrimental effect on the well-being of a child" is not defined in detail. Guidance is needed on addictive design, manipulative notifications, discriminatory profiling, exposure of location, harmful recommendations and commercial exploitation.

Sixth, educational institutions receive important monitoring exemptions. Without independent impact assessments and retention limits, schools may normalise continuous surveillance. Children should not be required to exchange privacy for access to education.

Finally, the DPDP framework primarily provides regulatory penalties. It does not establish a specialised statutory compensation system through which children can easily recover the costs of identity misuse, psychological support or removal of harmful data.

8. Comparative Approaches

The European Union's General Data Protection Regulation provides special protection for children and regulates consent for information-society services. The default age for independent consent is sixteen, although Member States may provide a lower threshold not below thirteen.

The EU Digital Services Act goes beyond consent by requiring platforms accessible to minors to provide high levels of privacy, safety and security. It prohibits targeted advertising to minors based upon profiling.



The United Kingdom's Children's Code contains fifteen age-appropriate design standards. It makes the child's best interests a primary consideration and emphasises high-privacy defaults, data minimisation, transparency and age-appropriate application.

The United States' COPPA framework places parents in control of information collected online from children under thirteen. The Federal Trade Commission strengthened the Rule in 2025, including tighter limits on monetisation and targeted advertising.

These models demonstrate that consent alone is insufficient. Design standards, profiling restrictions, regulatory supervision and enforceable default settings are equally important.

9. Recommendations for Constitutional and Legal Reform

India should develop a statutory **Children's Online Privacy and Age-Appropriate Design Code** under the DPDP framework. The code should make the child's best interests a primary consideration and translate general legal duties into practical design requirements.

Online services likely to be accessed by children should use high-privacy settings by default. Location sharing, public profiles, contact discovery and personalised advertising should remain disabled unless a mature child or parent makes an informed and reversible choice.

Data minimisation should be applied strictly. Schools and platforms should collect only the information necessary for a defined purpose. Children's information should not be retained merely because it may later become commercially useful.

Privacy notices should be presented in language, symbols and formats appropriate to different age groups. A notice designed for an adult cannot provide meaningful understanding to a child. India should adopt risk-based and privacy-preserving age assurance. Services should be permitted to receive an age-range confirmation without receiving full identity records wherever possible. Biometric age estimation should undergo independent testing for accuracy, discrimination and security.

Adolescents should receive an increasing role in consent and rights-exercise. Where processing is not necessary for protection from serious harm, the views of an older child should not be displaced automatically by parental preference. Children should be able to request access, correction and erasure through child-friendly procedures.

Educational technology should be governed by a separate code. Schools should conduct data-protection impact assessments before adopting tools that record behaviour, biometrics, location or communications. Contracts must prohibit advertising, unrelated commercial use and sale of student data.

The Data Protection Board should develop a specialised child-rights unit with expertise in education, developmental psychology, disability, platform design and cybercrime. Complaints submitted by children should receive priority and should not require complex legal drafting.

Independent audits should examine not only data security but also recommendation systems, addictive features, profiling and discriminatory outcomes. Audit summaries should be publicly available without exposing security-sensitive information.



Children must also participate in rule-making. International child-rights standards emphasise that their views should be given due weight. Consultation should include children from rural areas, linguistic minorities, low-income families and children with disabilities, not only technologically privileged students.

Finally, digital literacy should teach children how data are collected, inferred and commercialised. Responsibility must not be shifted entirely onto children, but informed participation can strengthen their ability to recognise manipulation and exercise legal rights.

10. Major Findings

The study finds that children's online privacy is protected constitutionally through dignity, liberty, equality, expression and development. It is not merely a consumer concern.

India's DPDP Act establishes significant child-specific safeguards, particularly the prohibition of behavioural monitoring and targeted advertising. Their delayed commencement, however, leaves a transitional protection gap until May 2027.

Parental consent is necessary for young children but cannot serve as the sole foundation of digital privacy. A rights-based framework must consider evolving capacities, confidential access and the possibility that parental monitoring may itself become excessive.

The greatest future challenge lies not in individual disclosure but in invisible data inference. Platforms can construct detailed profiles without asking children direct questions. Protection must therefore regulate design, algorithms and data combinations rather than focus only on consent forms.

11. Conclusion

Children's online privacy is a condition for dignity, intellectual development and meaningful participation in the digital world. A child who is continuously monitored, commercially profiled or permanently judged by early behaviour cannot exercise autonomy in the same way as a child allowed space to develop.

The Indian Constitution provides a strong normative foundation through the rights to equality, expression, education, dignity and privacy. Puttaswamy's recognition of informational privacy enables courts and regulators to examine not only government surveillance but also data-driven systems that shape identity and opportunity.

The DPDP Act and Rules represent substantial progress. Verifiable parental consent, restrictions on harmful processing and the prohibition of targeted advertising establish an important baseline. Yet protection will remain incomplete unless implementation addresses age-appropriate design, educational surveillance, privacy-preserving age assurance, child-accessible remedies and adolescent autonomy.

The objective should not be to exclude children from digital life. Excessive restriction can weaken education, expression and participation. The correct constitutional approach is to create a digital environment in which children can explore and learn without surrendering their identity, dignity and future to uncontrolled data collection.



References

- Committee on the Rights of the Child. (2021). *General Comment No. 25 on children's rights in relation to the digital environment*. United Nations.
- Constitution of India. (2026 ed.). Legislative Department, Ministry of Law and Justice, Government of India.
- Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
- Digital Personal Data Protection Rules, 2025.
- European Parliament and Council. (2016). *General Data Protection Regulation, Regulation (EU) 2016/679*.
- European Parliament and Council. (2022). *Digital Services Act, Regulation (EU) 2022/2065*.
- Federal Trade Commission. (2025). *Children's Online Privacy Protection Rule*.
- Information Technology Act, 2000, Act No. 21 of 2000.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2026.
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- Protection of Children from Sexual Offences Act, 2012, Act No. 32 of 2012.
- UNICEF. (2017). *Children's online privacy and freedom of expression: Industry toolkit*.
- UNICEF. (2024). *Data protection in schools: Guidance for legislators, policy makers and schools*.
- UNICEF. (2025). *Childhood in a digital world*.
- United Nations. (1989). *Convention on the Rights of the Child*.
- United Kingdom Information Commissioner's Office. (2020). *Age appropriate design: A code of practice for online services*.

Cite this Article:

Kumar, Dr. Surendra. (2026). Children's Online Privacy and Constitutional Protection: An Indian Legal Perspective in the Age of Data-Driven Platforms. The Research Dialogue, Open Access Peer-reviewed & Refereed Journal, Pp.324–334, Volume-04, Issue-04, January-2026, <https://theresearchdialogue.com/>



This is an Open Access Journal / article distributed under the terms of the Creative Commons Attribution License CC BY-NC-ND 3.0) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. All rights reserved.



CERTIFICATE

of Publication

This Certificate is proudly presented to

Dr. Surendra Kumar

For publication of Research Paper title

Children's Online Privacy and Constitutional Protection: An Indian Legal Perspective in the Age of Data-Driven Platforms

Published in 'The Research Dialogue' Peer-Reviewed / Refereed Research Journal and E-ISSN: 2583-438X, Volume-04, Issue-04, Month January, Year-2026, Impact Factor (RPRI-4.73)

Dr. Lohans Kumar Kalyani
Editor- In-chief



Dr. Neeraj Yadav
Executive-In-Chief- Editor

Note: This E-Certificate is valid with published paper and the paper must be available online at: <https://theresearchdialogue.com/>
DOI: <https://doi.org/10.64880/theresearchdialogue.v4i4.31>