



PURC Journal of Law,

Vol. 2, Issue 1, January - June, 2026, pp. 103-117

Artificial Intelligence and Child Rights in India: Addressing Online Safety, Privacy and Regulatory Challenges in the Digital Age

Ajitabh Mishra¹

Abstract

Artificial Intelligence (AI) has become deeply embedded in the digital lives of children, influencing the ways in which they learn, communicate, access information, play, and participate in online spaces. AI-powered educational applications, recommendation systems, social media platforms, online games, virtual assistants, and generative AI tools offer considerable opportunities for learning, creativity, accessibility, and social participation. At the same time, their growing use has created serious concerns relating to children's privacy, behavioural profiling, algorithmic discrimination, exposure to harmful content, online exploitation, deepfakes, and psychological well-being. These concerns acquire particular significance because children, owing to their age and evolving capacities, may be disproportionately affected by automated and data-driven systems whose functioning is often difficult to understand or challenge. This paper examines these emerging concerns through a doctrinal and comparative legal approach, drawing upon constitutional provisions, legislation, judicial decisions, international child-rights instruments, regulatory frameworks, and relevant empirical and policy reports. Particular attention is given to the guarantees of equality, non-discrimination, privacy, dignity, and personal liberty under Articles 14, 15 and 21 of the Constitution of India and their relevance to algorithmic decision-making affecting children. The paper critically evaluates the adequacy of the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, and the Digital Personal Data Protection Act, 2023 in responding to AI-enabled risks. It also considers the United Nations Convention on the Rights of the Child and comparative regulatory developments, particularly the European Union Artificial Intelligence Act. The central argument of the paper is that India's existing legal framework provides important protections against particular digital harms but does not yet adequately address the design, deployment, transparency, discriminatory effects, and accountability of AI systems affecting children. It therefore advocates a child-centred and constitutionally grounded approach to AI governance that combines technological innovation with privacy, equality, safety, transparency, accountability, and the best interests of the child.

Keywords: Artificial Intelligence; Child Rights; Online Safety; Digital Privacy; Algorithmic Discrimination; AI Governance; Constitutional Rights.

¹ Rayat College of Law, Railmajra (Affiliated to Panjab University), Panjab, India. Email: profajitabh@gmail.com

Introduction

Artificial Intelligence (AI) has emerged as one of the most significant technological developments shaping contemporary society. What was once largely confined to specialised technological applications has gradually become part of ordinary digital life through search engines, social media platforms, online games, educational applications, virtual assistants, recommendation systems and, more recently, generative AI tools. Children encounter these systems while studying, communicating, creating content, playing games and accessing entertainment. Consequently, their engagement with artificial intelligence often begins long before they are capable of fully understanding how algorithmic systems collect information, make predictions or influence the digital content presented to them.²

The increasing integration of AI into childhood presents both opportunities and risks. AI-assisted educational platforms can personalise learning, improve accessibility and provide students with immediate educational support. Generative AI can facilitate creativity and access to information, while intelligent technologies may assist children with disabilities and overcome certain linguistic and geographical barriers. At the same time, the same technological capabilities can expose children to extensive data collection, behavioural profiling, manipulative design practices, harmful recommendations and new forms of online exploitation. UNICEF has therefore emphasised that AI systems affecting children should be designed and deployed in a manner that supports their development and well-being while protecting privacy, fairness, safety and non-discrimination.³

The scale of children's participation in the digital environment makes these concerns more than theoretical. International evidence demonstrates that internet access has become an important part of childhood across the world, although access remains deeply unequal. UNICEF and the International Telecommunication Union estimated that approximately **two-thirds of school-age children worldwide did not have an internet connection at home** in 2020, revealing a significant digital divide alongside the rapid expansion of digital technologies.⁴ Such inequality acquires a new dimension in the age of AI. Children with reliable connectivity and access to advanced digital tools may benefit from personalised education and information, whereas children belonging to economically or socially disadvantaged communities may experience technological exclusion. At the same time, increased connectivity can create additional exposure to privacy violations, cyber exploitation, harmful content and algorithmically amplified risks. The challenge, therefore, is not simply to increase children's access to technology but to ensure that such access is safe, equitable and consistent with their rights.

Artificial intelligence also changes the character of traditional online risks. Earlier approaches to internet regulation generally concentrated on unlawful content, cybercrime, privacy breaches and misconduct committed by identifiable individuals. AI-driven environments are

² Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–12 (Pearson Education, 4th edn., 2021).

³ United Nations Children's Fund (UNICEF), *Policy Guidance on AI for Children* 14–20 (UNICEF, 2021).

⁴ UNICEF and International Telecommunication Union, *How Many Children and Young People Have Internet Access at Home? Estimating Digital Connectivity During the COVID-19 Pandemic* 5–7 (UNICEF, New York, 2020).

considerably more complex. Recommendation algorithms can determine which information children repeatedly encounter; predictive systems can construct detailed profiles from their online behaviour; generative AI can create realistic synthetic images, audio and video; and automated systems may make decisions without providing meaningful explanations to affected individuals. These technologies can therefore influence children even where no immediate unlawful act is visible. The resulting harm may arise from the architecture and operation of the technological system itself rather than from a single identifiable act of misconduct.⁵

Article 21 provides an equally important constitutional foundation. The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognised privacy as a constitutionally protected fundamental right associated with dignity, liberty and individual autonomy.⁶ In an AI-driven environment, this protection extends beyond secrecy or unauthorised disclosure of information. Children's digital activities generate extensive data concerning their interests, communications, location, behaviour and preferences. When such information is continuously collected, combined and analysed by algorithms, questions arise regarding informational privacy, autonomy and the ability of children to exercise meaningful control over their digital identities. The constitutional principles recognised in *Puttaswamy* therefore provide an essential normative basis for evaluating AI-driven profiling and surveillance.

The equality dimension is equally important because technological systems are not necessarily neutral merely because decisions are produced through automated processes. AI models learn from data drawn from existing social environments, and such data may reflect historical inequalities and discriminatory practices. If these patterns enter automated decision-making, technological systems can reproduce or even intensify existing disadvantage. This concern is particularly significant in India because caste, gender, economic status, language, disability and unequal access to technology may intersect with children's experiences in the digital environment. Algorithmic discrimination should therefore be examined not merely as a technical defect in software but as a potential constitutional concern involving equality, dignity and substantive non-discrimination.⁷

International child-rights law reinforces this constitutional approach. The United Nations Convention on the Rights of the Child (UNCRC) requires the best interests of the child to remain a primary consideration in actions affecting children and protects their rights to participation, privacy, development and protection from exploitation.⁸ The UN Committee on the Rights of the Child has subsequently clarified that these rights apply fully within the digital environment and that States must take appropriate measures to ensure that

⁵ United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* 17–22 (UNESCO, Paris, 2021).

⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁷ NITI Aayog, *Responsible AI #AIForAll: Approach Document for India, Part 1 – Principles for Responsible AI* 25–34 (Government of India, New Delhi, 2021).

⁸ United Nations Convention on the Rights of the Child, 1989, arts. 3, 12, 16, 17 and 19.

technological developments do not undermine children's rights.⁹ These principles are increasingly important as artificial intelligence determines what children see, how their behaviour is analysed and how digital services interact with them.

Against this background, **this paper argues that India's existing legal framework provides important remedies against particular forms of digital harm but remains insufficiently equipped to regulate the design, deployment, transparency and accountability of AI systems affecting children.** The central concern is therefore not the absence of legal protection altogether, but the gap between laws primarily designed to respond to identifiable harms and AI systems capable of producing systemic, predictive and sometimes discriminatory consequences. The paper contends that Articles 14, 15 and 21 of the Constitution, read alongside the UNCRC and emerging comparative regulatory standards such as the EU AI Act, can provide the normative foundation for a more coherent child-centred framework of AI governance. Such an approach must preserve the educational and developmental benefits of artificial intelligence while ensuring that innovation does not come at the cost of children's equality, privacy, dignity, safety and best interests.

Research Methodology

This study adopts a **doctrinal legal research methodology** to examine the implications of artificial intelligence for child rights in India. The analysis is primarily based on constitutional provisions, statutory enactments, judicial decisions and international legal instruments relevant to children's privacy, equality, dignity and online safety. Particular attention is given to Articles 14, 15 and 21 of the Constitution of India, the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, and the Digital Personal Data Protection Act, 2023. Judicial decisions, particularly *Justice K.S. Puttaswamy (Retd.) v. Union of India*, are examined to understand the constitutional application of privacy, dignity and individual autonomy in technology-mediated environments.¹⁰

Artificial Intelligence and the Changing Digital Environment for Children

Artificial intelligence has changed children's relationship with digital technology from relatively passive internet use to continuous interaction with systems capable of predicting preferences, generating content and shaping choices. Search engines, educational applications, social-media feeds, online games and conversational assistants increasingly operate through machine-learning models that analyse user behaviour and modify subsequent interactions. For children, therefore, AI is often encountered not as a separate technological product but as an invisible layer operating within services they already use.¹¹

A. Growing Interaction of Children with AI

⁹ UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc. CRC/C/GC/25, paras. 12–21, 67–78 (2021).

¹⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

¹¹ United Nations Children's Fund (UNICEF), *Policy Guidance on AI for Children* 10–16 (UNICEF, 2021).

The extent of this interaction is becoming measurable. Recent UNICEF research based on data from ten countries estimates that **at least 20 million children have used AI**, with children adopting these technologies at rates more than three times those of their parents or caregivers. Approximately **13 million children in the study used AI for learning or homework**, while more than **two million—around one in ten—reported using AI for advice about matters that worried them**.¹² Although these findings should not be treated as global prevalence estimates, they demonstrate that AI has already entered areas of childhood extending beyond entertainment into education and personal decision-making.

AI-assisted education illustrates its potential benefits. Intelligent tutoring systems can adapt learning materials to individual performance, assist with translation, provide immediate feedback and improve accessibility for children with disabilities. UNICEF reported that in 2025 more than **13.6 million children across 71 countries accessed education through digital platforms supported by the organisation**, while AI-powered accessible digital textbooks developed by fourteen governments reached nearly **two million children**.¹³ Such applications demonstrate that responsible AI can contribute to educational inclusion rather than merely creating regulatory risk.

Generative AI has further transformed children's digital experiences. Unlike conventional recommendation systems, generative models can produce text, images, audio, video and computer code in response to user instructions. Their conversational character can make interaction appear personalised and authoritative, even where the generated information is inaccurate. UNESCO has consequently recommended an age-appropriate and human-centred approach to generative AI in education, including protection of personal data and appropriate age restrictions for independent interaction with such systems.¹⁴

B. Algorithmic Personalisation and Behavioural Profiling

Recommendation systems constitute another important form of everyday AI interaction. Social-media, video-sharing, streaming and gaming platforms analyse searches, viewing history, clicks, purchases and engagement patterns to determine what a user is likely to watch or interact with next. Personalisation may make digital services more useful, but it also means that a child's information environment can be shaped by automated predictions that remain largely invisible to the child.

This process is particularly significant because **data collection, profiling and recommendation operate as an interconnected mechanism**. A platform first collects information about a child's activities; algorithms then identify patterns and construct a behavioural profile; that profile subsequently influences the content, advertisements or recommendations presented to the child. Repeated interaction generates additional data,

¹² UNICEF Office of Strategy and Evidence–Innocenti, *Snapshot of AI Usage and Concerns Among Children and Parents: Insights from 10 Countries* (2026); UNICEF, “Children are Adopting AI Technologies More Than Three Times Faster Than Adults,” Statement, June 30, 2026.

¹³ UNICEF, *Annual Report 2025: Continuing to Deliver for Children, in Crises and Beyond* (2026).

¹⁴ Fengchun Miao and Wayne Holmes, *Guidance for Generative AI in Education and Research* 21–28 (UNESCO, Paris, 2023).

allowing the system to refine its predictions. The result is a continuing feedback loop in which children's past behaviour increasingly influences their future digital environment.¹⁵

C. From Digital Opportunity to Algorithmic Vulnerability

Children's particular vulnerability arises from the combination of intensive data processing and their evolving capacity to understand persuasive technologies. Personalisation can improve educational and entertainment experiences, yet the same mechanisms can encourage prolonged engagement, facilitate targeted influence and repeatedly expose users to particular categories of content. Generative systems add further concerns relating to fabricated information, synthetic identities and realistic manipulated images.

The central regulatory issue is therefore not simply whether children should use artificial intelligence. AI already provides meaningful educational and accessibility benefits, and its use among children is expanding rapidly. The more important question is **how AI systems affecting children are designed, trained and deployed, what information they collect, and whether meaningful safeguards exist against discriminatory, manipulative or unsafe outcomes.**

Child Rights Framework and AI Governance

The emergence of artificial intelligence does not require the creation of an entirely new category of rights for children. Rather, it requires established constitutional and child-rights guarantees to be applied to technological systems capable of collecting data, predicting behaviour and influencing opportunities. In India, Articles 14, 15 and 21 provide an important constitutional foundation for examining algorithmic discrimination, privacy and autonomy, while international child-rights standards supply additional principles of best interests, participation and protection.

A. Equality, Non-Discrimination and Algorithmic Bias

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws. The Supreme Court has consistently treated arbitrariness as incompatible with equality. In *E.P. Royappa v. State of Tamil Nadu*, the Court recognised that equality and arbitrariness are fundamentally opposed.¹⁶ This principle assumes renewed importance where decisions affecting individuals are increasingly assisted or produced by algorithms. An automated outcome cannot be regarded as fair merely because it has been generated technologically; the underlying data, criteria and consequences must also withstand constitutional scrutiny.

Article 15 adds a specific non-discrimination dimension by prohibiting discrimination on grounds including religion, race, caste, sex and place of birth. AI systems may create difficulties in this context because discrimination need not be expressly programmed into an algorithm. Bias can enter through **training data, classification and proxy variables**. If historical data reflect existing social inequalities, a model trained on those data may learn the same patterns. Even where caste is not directly recorded, variables such as surname, locality,

¹⁵ United Nations Children's Fund (UNICEF), *Policy Guidance on AI for Children*, supra note 15, at 20–24.

¹⁶ *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.

language, school attended or socio-economic circumstances may operate as proxies and produce outcomes correlated with caste or social position.¹⁷

The Supreme Court's movement towards **substantive equality** provides useful guidance. In *Navtej Singh Johar v. Union of India*, the Court emphasised constitutional morality, dignity and protection against discrimination rather than merely formal equality.¹⁸ Applied to AI, this approach requires regulators to examine the real effects of automated systems on vulnerable groups, including children, rather than assuming technological neutrality.

B. Privacy, Dignity and Autonomy under Article 21

Artificial intelligence also raises significant concerns under **Article 21**, particularly because contemporary AI systems depend heavily upon personal data. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge Bench of the Supreme Court recognised privacy as a fundamental right intrinsic to life and personal liberty and closely connected with dignity and autonomy.¹⁹ The judgment is particularly relevant to children's digital rights because AI-enabled services can collect information about browsing behaviour, communications, location, interests, educational performance and personal preferences.

Article 21 must also be read with **Article 21A**, which guarantees free and compulsory education to children between six and fourteen years. As AI becomes integrated into education, technological innovation should promote rather than deepen educational inequality. Articles **39(e)** and **39(f)** further reinforce the State's responsibility to protect children against exploitation and ensure conditions conducive to healthy development and dignity.²⁰

C. International Child-Rights Standards

The **United Nations Convention on the Rights of the Child (UNCRC)** provides a complementary rights-based framework. Article 3 requires the best interests of the child to be a primary consideration, Article 12 protects participation, Article 16 safeguards privacy and Articles 19 and 34 require protection against violence and sexual exploitation.²¹ These guarantees apply equally in digital environments. The UN Committee on the Rights of the Child, through **General Comment No. 25**, has specifically recognised that children's rights must be respected, protected and fulfilled in relation to digital technologies and has emphasised privacy, non-discrimination, safety and age-appropriate design.²²

The best-interests principle is especially important for AI governance. A platform designed primarily to maximise engagement or commercial returns may not necessarily operate in children's best interests. Child-sensitive governance therefore requires safety and

¹⁷ NITI Aayog, *Responsible AI #AIForAll: Approach Document for India, Part 1 – Principles for Responsible AI* 25–34 (Government of India, New Delhi, 2021).

¹⁸ *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.

¹⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

²⁰ The Constitution of India, arts. 21A, 39(e) and 39(f).

²¹ United Nations Convention on the Rights of the Child, 1989, arts. 3, 12, 16, 19 and 34.

²² UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc. CRC/C/GC/25, paras. 9–14, 23–36, 67–78 (2021).

developmental considerations to influence technological design before harm occurs rather than relying exclusively upon remedies after injury.

D. Comparative Regulatory Approaches and Lessons for India

Comparative developments demonstrate an increasing shift towards preventive regulation. The **European Union Artificial Intelligence Act, 2024** adopts a risk-based framework under which regulatory obligations increase according to the potential impact of an AI system. Of particular relevance to children, Article 5 prohibits specified manipulative or deceptive AI practices and certain practices exploiting vulnerabilities arising from age, disability or particular social or economic situations where the statutory conditions concerning distortion of behaviour and significant harm are satisfied.²³ The Act therefore recognises that vulnerability can arise from the relationship between technological design and the characteristics of particular users.

The **United Kingdom's Age Appropriate Design Code** similarly requires online services likely to be accessed by children to place their best interests at the centre of design decisions and incorporates safeguards concerning profiling, geolocation, transparency and privacy-protective default settings.²⁴ These approaches differ in form but share an important principle: child protection should influence the **design and deployment** of technology rather than begin only after harm has occurred.

Online Safety Challenges for Children in the Age of AI

Artificial intelligence has altered both the scale and character of online risks faced by children. Conventional concerns such as privacy breaches, cyberbullying and inappropriate content continue to exist, but AI adds new dimensions through automated profiling, synthetic media, personalised recommendations and increasingly human-like conversational systems. These risks are particularly significant for children because technological systems can influence their behaviour or use their personal information without the process being readily visible or understandable.

A. Data Collection, Profiling and Algorithmic Influence

AI-based services depend extensively upon data. Searches, viewing patterns, location information, online purchases, educational activity and interactions with digital content can be combined to construct detailed behavioural profiles. Such profiles allow platforms to predict interests and personalise recommendations, but they also create concerns about children's privacy and autonomy. UNICEF's updated guidance on AI and children consequently identifies protection of children's data and privacy, non-discrimination, transparency and explainability among the core requirements of child-centred AI.²⁵

²³ Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), art. 5.

²⁴ Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* (United Kingdom, 2020).

²⁵ UNICEF Office of Strategy and Evidence–Innocenti, *Guidance on AI and Children: Recommendations for AI Policies and Systems that Uphold Child Rights*, Version 3.0 (UNICEF, 2025).

The concern is greater where personalisation becomes behavioural influence. Recommendation algorithms generally learn from previous interactions and provide content likely to maintain engagement. This can create a feedback loop in which a child who interacts with a particular category of material is repeatedly shown similar content. For younger users who may have limited ability to recognise persuasive design, the distinction between useful personalisation and manipulation can become difficult to identify. The risk therefore arises not only from what information is collected but also from **how predictions derived from that information subsequently shape children's choices.**

B. Deepfakes, Synthetic Content and Sexual Exploitation

Generative AI has considerably lowered the technical barriers to creating realistic synthetic images, audio and video. Deepfake technology can manipulate an ordinary photograph of a child into fabricated sexualised material without any physical contact with the victim. The scale of this emerging problem is now supported by empirical evidence. A 2026 study undertaken through the UNICEF, ECPAT International and INTERPOL *Disrupting Harm* project across eleven countries found that **at least 1.2 million children reported that their images had been manipulated into sexually explicit deepfakes during the preceding year.** In some surveyed countries, the prevalence was approximately **one in twenty-five children.**²⁶

Evidence from content-monitoring organisations demonstrates a similarly rapid technological escalation. The Internet Watch Foundation recorded **491 reports containing realistic AI-generated child sexual abuse imagery in 2025,** compared with 193 in 2024, an increase of 154 per cent. More strikingly, it identified **3,443 AI-generated child sexual abuse videos in 2025 compared with only 13 in 2024.**²⁷ These figures do not establish the overall global prevalence of such material, but they demonstrate how quickly generative tools can expand the capacity to produce realistic abusive content.

AI-generated material creates legal and practical difficulties even where the image is synthetic. A real child's photograph may be used as source material, fabricated content can be employed for harassment or extortion, and increasing volumes of synthetic material may complicate efforts by law-enforcement agencies to identify children experiencing physical abuse. UNICEF has accordingly emphasised that AI-generated sexual abuse and exploitation should be treated as a serious child-protection concern rather than dismissed because an image has been technologically produced.²⁸

C. AI-Enabled Grooming, Impersonation and Conversational Systems

AI can also increase the sophistication of deceptive online interaction. Generative systems can produce convincing photographs, synthetic voices and personalised messages, enabling offenders to construct false identities with greater ease. Such tools may facilitate grooming,

²⁶ UNICEF, *Artificial Intelligence and Child Sexual Abuse and Exploitation*, Issue Brief 3–4 (Feb. 2026); UNICEF, ECPAT International and INTERPOL, *Disrupting Harm*, as reported therein.

²⁷ Internet Watch Foundation, *Annual Data & Insights Report 2025: AI-Generated Child Sexual Abuse Material* (2026).

²⁸ UNICEF, *Artificial Intelligence and Child Sexual Abuse and Exploitation*, supra note 30, at 3–6.

impersonation and sexual extortion by making deceptive communication appear more credible.

Conversational AI raises a related but distinct concern. UNICEF's 2026 evidence from ten countries estimated that **more than two million children—approximately one in ten of the children represented in the study—used AI for advice about matters that worried them.**²⁹ This does not mean that conversational AI is inherently harmful; such systems may provide useful information and support. It does, however, demonstrate that some children are using AI in emotionally significant contexts. Inaccurate, manipulative or developmentally inappropriate responses can therefore have consequences extending beyond ordinary informational error.

D. Harmful Content and Psychological Well-Being

AI-powered recommendation systems can also influence children's exposure to violent, discriminatory, misleading or otherwise harmful content. The problem lies partly in amplification. Systems optimised for engagement may repeatedly recommend material similar to content with which a user has previously interacted, potentially narrowing the child's information environment and reinforcing harmful patterns.

The emerging evidence demonstrates that AI does more than intensify familiar internet risks. It enables harmful material to be generated at scale, allows existing images to be transformed into abusive content, facilitates sophisticated impersonation and gives automated systems an increasingly influential role in children's informational and emotional environments. Effective online safety regulation must therefore address not only harmful users and unlawful content but also the **design features, data practices and algorithmic processes that can create or amplify harm before conventional legal remedies are triggered.**

Evaluating India's Regulatory Response

India does not presently regulate artificial intelligence affecting children through a single comprehensive statute. Protection instead emerges from a combination of cyber law, data-protection legislation, criminal law and constitutional guarantees. The Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and the Protection of Children from Sexual Offences Act, 2012 address important aspects of children's digital safety, but each approaches the problem from a different regulatory perspective. The central difficulty is that these laws primarily regulate data processing, unlawful content or prohibited conduct, whereas many AI-related risks originate earlier, in the design, training and deployment of algorithmic systems.

A. Information Technology Act, 2000 and Platform Regulation

The **Information Technology Act, 2000** remains an important foundation of India's cyber-law framework. Provisions concerning unauthorised access, identity-related offences, cheating by personation and sexually explicit material provide remedies against several forms

²⁹ UNICEF Office of Strategy and Evidence—Innocenti, *Snapshot of AI Usage and Concerns Among Children and Parents: Insights from 10 Countries* (June 2026).

of online misconduct. Section 67B is particularly relevant to children because it criminalises specified activities involving electronic material depicting children in sexually explicit acts or conduct.³⁰ These provisions can apply to technology-facilitated exploitation even though the legislation predates contemporary generative AI.

The Act nevertheless has structural limitations when applied to artificial intelligence. It was not designed to examine algorithmic profiling, discriminatory models, automated recommendations or the training data used by AI systems. The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**, as amended, impose due-diligence obligations upon intermediaries and establish mechanisms concerning unlawful online content.³¹ Such mechanisms are significant for child safety, but content moderation alone cannot address risks produced by the underlying architecture of an AI system. Removing harmful content after publication, for example, does not resolve questions concerning why an algorithm repeatedly recommended such material to a child.

B. Digital Personal Data Protection Framework and Children's Data

The **Digital Personal Data Protection Act, 2023 (DPDP Act)** represents a more direct attempt to protect children in data-intensive environments. Section 9 establishes special obligations regarding the processing of children's personal data. It requires verifiable parental consent before such processing, subject to the statutory framework and applicable exemptions, and prohibits processing that is likely to cause a detrimental effect on the well-being of a child. It also restricts tracking or behavioural monitoring of children and targeted advertising directed at them, subject to the manner in which the Act and applicable rules or exemptions operate.³²

However, parental consent by itself cannot resolve every AI-related privacy concern. Parents may not fully understand complex data-processing practices, while children may use services across several devices and platforms. Moreover, consent does not necessarily provide meaningful information about how an AI model subsequently derives inferences from collected data. The regulatory challenge therefore extends beyond obtaining permission to ensuring **purpose limitation, data minimisation, transparency and accountability throughout the technological lifecycle**.

A further issue concerns the Act's general treatment of persons below eighteen years as children.³³ A uniform threshold provides clear protection but may not always reflect children's evolving capacities. The informational needs and digital autonomy of a seventeen-year-old, for example, differ considerably from those of a young child. Child protection must therefore be sufficiently strong without unnecessarily preventing older adolescents from accessing beneficial digital services.

C. POCSO and AI-Facilitated Sexual Exploitation

³⁰ Information Technology Act, 2000, ss. 43, 66C, 66D and 67B.

³¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.

³² Digital Personal Data Protection Act, 2023, s. 9.

³³ *Id.*, s. 2(f).

The **Protection of Children from Sexual Offences Act, 2012 (POCSO)** remains central where artificial intelligence is used to facilitate sexual exploitation. Sections 13 to 15 address the use of children for pornographic purposes and related storage or possession of pornographic material involving children.³⁴ The legislation can consequently operate alongside the IT Act where digital technologies are used to exploit children.

Generative AI nevertheless creates interpretative challenges that were not contemplated when POCSO was enacted. Synthetic sexual material may involve a recognisable real child whose image has been manipulated, entirely artificial representations, or combinations of real and generated content. As demonstrated by the empirical evidence discussed earlier, AI-generated abusive imagery is expanding rapidly. Indian law therefore requires sufficient clarity to ensure that technological changes in the method of producing exploitative material do not create uncertainty in protection, investigation or prosecution.

The Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish*³⁵ is important in this context. In 2024, the Court emphasised the seriousness of child sexual exploitative and abuse material and recommended replacing the expression “child pornography” with terminology reflecting the exploitative and abusive nature of such material.³⁶ The judgment reinforces the principle that digital child protection must focus upon exploitation and harm rather than treating such material merely as obscene content.

D. Regulatory Gaps and the Way Forward

Taken together, the existing laws provide significant but fragmented protection. The IT framework addresses cyber offences, intermediaries and unlawful content; the DPDP framework regulates processing of children's personal data; and POCSO targets sexual exploitation. What remains comparatively underdeveloped is regulation of **AI systems as systems**. Indian law does not yet provide a comprehensive child-specific mechanism requiring systematic assessment of algorithmic bias, explainability, risk classification or child-rights impact before high-risk AI applications are deployed.

This gap does not necessarily require India to reproduce the European Union's regulatory model in its entirety. Indian AI governance must respond to domestic constitutional conditions, technological capacity and socio-economic realities. Nevertheless, the preventive logic underlying comparative approaches offers useful guidance. AI systems substantially affecting children could be subjected to **child-rights impact assessments**, periodic testing for discriminatory outcomes, privacy-protective default settings and enhanced transparency obligations. High-risk applications involving education, biometric identification or access to essential public services may justify stronger scrutiny.

Concluding Reflections

Artificial intelligence is increasingly becoming part of the environment in which children learn, communicate, seek information and develop social relationships. Its growing presence

³⁴ Protection of Children from Sexual Offences Act, 2012, ss. 13–15.

³⁵ (2024) INSC 716

³⁶ *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716.

offers considerable possibilities for personalised education, accessibility, creativity and participation. At the same time, the analysis in this paper demonstrates that AI introduces risks that cannot be adequately understood through the traditional framework of internet safety alone. Behavioural profiling, algorithmic discrimination, synthetic sexual content, automated recommendations and AI-enabled impersonation illustrate how harm may originate not merely from individual misuse of technology but also from the manner in which AI systems are designed, trained and deployed.

The constitutional analysis further demonstrates that these concerns are fundamentally questions of rights. Article 14 requires protection against arbitrary and unequal technological outcomes, while Article 15 becomes relevant where automated systems reproduce disadvantages associated with caste, sex or other constitutionally protected grounds. Article 21, particularly after *Justice K.S. Puttaswamy (Retd.) v. Union of India*, provides a strong foundation for protecting children's privacy, dignity and autonomy against disproportionate data collection and profiling. Read together with the UNCRC's principles of best interests, participation and protection, these guarantees provide a normative foundation for child-centred AI governance in India.

India is therefore not starting from a position of legal absence. The Information Technology Act, 2000, the POCSO Act, 2012 and the Digital Personal Data Protection Act, 2023 already provide significant safeguards against cyber misconduct, sexual exploitation and misuse of children's personal data. The difficulty lies in their **fragmented and predominantly reactive character**. They respond more readily to identifiable misconduct or resulting harm than to risks embedded within algorithmic design, training data, automated profiling and decision-making. This regulatory gap becomes increasingly significant as AI systems assume a greater role in children's educational and social environments.

Ultimately, the question is not whether children should participate in an AI-driven society; that transformation is already underway. The more important question is whether technological development will occur on terms that respect their rights and evolving capacities. India's constitutional commitment to equality, dignity, privacy and child welfare provides the principles necessary to answer that question. The task ahead is to translate those principles into enforceable safeguards capable of ensuring that artificial intelligence develops for children without developing at the expense of their rights.

BIBLIOGRAPHY

Books

- Haidt, Jonathan, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (Penguin Press, New York, 2024).
- Hartzog, Woodrow, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, Cambridge, 2018).

- Holmes, Wayne and Maya Bialik, *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning* (Center for Curriculum Redesign, Boston, 2019).
- Livingstone, Sonia and Alicia Blum-Ross, *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives* (Oxford University Press, Oxford, 2020).
- Palfrey, John and Urs Gasser, *Born Digital: How Children Grow Up in a Digital Age* (Basic Books, New York, rev. edn., 2016).
- Russell, Stuart and Peter Norvig, *Artificial Intelligence: A Modern Approach* (Pearson Education, 4th edn., 2021).
- Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, London, 2019).

Reports, Policy Documents and Institutional Publications

- Indian Cyber Crime Coordination Centre (I4C), *Cyber Crime Trends Report 2023* (Ministry of Home Affairs, Government of India, 2024).
- Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* (United Kingdom, 2020).
- Internet Watch Foundation, *Annual Data & Insights Report 2025: AI-Generated Child Sexual Abuse Material* (2026).
- NITI Aayog, *Responsible AI #AIForAll: Approach Document for India, Part 1 – Principles for Responsible AI* (Government of India, New Delhi, 2021).
- Organisation for Economic Co-operation and Development (OECD), *Children in the Digital Environment: Revised Recommendation* (OECD, 2021).
- Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Artificial Intelligence* (OECD, 2019).
- UNICEF and International Telecommunication Union, *How Many Children and Young People Have Internet Access at Home? Estimating Digital Connectivity During the COVID-19 Pandemic* (UNICEF, New York, 2020).
- UNICEF Office of Strategy and Evidence–Innocenti, *Guidance on AI and Children: Recommendations for AI Policies and Systems that Uphold Child Rights*, Version 3.0 (UNICEF, 2025).
- UNICEF Office of Strategy and Evidence–Innocenti, *Snapshot of AI Usage and Concerns Among Children and Parents: Insights from 10 Countries* (UNICEF, 2026).
- United Nations Children's Fund (UNICEF), *Artificial Intelligence and Child Sexual Abuse and Exploitation*, Issue Brief (UNICEF, 2026).
- United Nations Children's Fund (UNICEF), *Annual Report 2025: Continuing to Deliver for Children, in Crises and Beyond* (UNICEF, 2026).
- United Nations Children's Fund (UNICEF), *Policy Guidance on AI for Children* (UNICEF, 2021).
- United Nations Educational, Scientific and Cultural Organization (UNESCO), *Guidance for Generative AI in Education and Research* (UNESCO, Paris, 2023).

- United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, Paris, 2021).

International Instruments and Standards

- Convention on the Rights of the Child, 1989.
- UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc. CRC/C/GC/25 (2021).
- Universal Declaration of Human Rights, 1948.

Cases

- *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716.
- *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.
- *Society for Unaided Private Schools of Rajasthan v. Union of India*, (2012) 6 SCC 1.
- *Unni Krishnan, J.P. v. State of Andhra Pradesh*, (1993) 1 SCC 645.

Indian Legislation

- The Constitution of India.
- Digital Personal Data Protection Act, 2023.
- Information Technology Act, 2000.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
- Protection of Children from Sexual Offences Act, 2012.

Foreign and Comparative Legislation

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Websites and Institutional Resources

- Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India.
- Information Commissioner's Office, United Kingdom.
- Internet Watch Foundation.
- NITI Aayog, Government of India.
- Organisation for Economic Co-operation and Development (OECD).
- United Nations Children's Fund (UNICEF).
- United Nations Educational, Scientific and Cultural Organization (UNESCO).