

Artificial Intelligence and Child Protection in India: Emerging Constitutional and Legal Challenges

Ms. Nasima Aktara Choudhury

Research Scholar, Law, Assam University

ABSTRACT

Children today are growing up in a world where digital technologies are woven into everyday life, shaping how they learn, interest and express themselves. While this has created new opportunities, yet it has also exposed children to less visible but deeply concerning forms of harm, particularly those emerging in online spaces. In the Indian context, the increasing use of social media platforms, digital applications, and Artificial intelligence has raised serious questions about how effectively the law is able to safeguard children's privacy and ensure their safety in such environments. Although the Constitution of India provides a strong foundation for the protection of fundamental rights, its application to the realities of digital childhood remains uneven and, at times, inadequate.

This paper seeks to explore how constitutional principles can respond to the growing challenges of protecting children online, especially in cases involving cyber grooming, sextortion, cyber bullying, and the misuse or circulation of personal data without consent. Using a doctrinal and analytical approach, the study examines constitutional provisions, relevant judicial developments, and existing statutory framework, including the Protection of Children from Sexual Offences Act, 2012, to understand their capacity to address these evolving harms. It also reflects on the delicate balance between safeguarding children and preserving fundamental freedoms, particularly the right to privacy under Article 21 and freedom of expression under Article 19.

The paper highlights a key gap in the current legal framework-while laws exist, they are largely shaped by offline perspective of harm and therefore struggle to keep pace with the fluid and borderless nature of digital abuse. Issues such as anonymity of offenders, algorithm-driven targeting, and limited accountability of digital platforms further complicate effective enforcement. In this context, the study argues that shift in approach is necessary-one that recognizes children not merely as passive recipients of protection but as rights-bearing individuals within the digital ecosystem.

The paper concludes by suggesting the need for a more nuanced and forward-looking constitutional responses that brings together child protection and digital governance, It emphasizes the importance of clearer accountability mechanisms, Child-sensitive regulatory standards, and a stronger commitment to protecting children's dignity, privacy and safety in an increasingly technology-driven world.

Keywords: Child Rights, Online Abuse, Privacy, Digital Safety, Artificial Intelligence, Cyber Exploitation

INTRODUCTION

The idea of child rights has long focused on safeguarding children from physical abuse, neglect, exploitation, and harm, while also ensuring their access to education, healthcare, and basic social support. Today, however, the rapid growth of digital technology has transformed the world in which children grow up, learn, and communicate. In modern India, children are deeply engaged with digital spaces—using online learning platforms, social media, gaming apps, and even AI-based tools from a very early age. While these innovations create valuable opportunities, they also bring a new set of risks that traditional systems of child protection were not designed to handle.¹

The digital environment has blurred the line between public and private life, exposing children to dangers that are often hidden, cross-border, and technologically complex. Issues such as online sexual exploitation, cyber grooming, harmful or inappropriate content, cyberbullying, identity theft, and the misuse of personal data have become pressing concerns. Unlike conventional forms of abuse, these threats frequently occur outside the immediate supervision of parents, teachers, or authorities, making them harder to detect and address.

In India, the Constitution reflects a strong commitment to the welfare, protection, and dignity of children. However, these ideals were shaped in a time before the rise of digital technologies and now need to be reinterpreted in light of new realities. The legal system faces the dual challenge of adapting existing child protection laws to the online world while also creating forward-looking regulations that can keep pace with rapidly evolving technological change.²

CHILDREN AND THE DIGITAL ENVIRONMENT

Children and young people today are among the most active participants in the digital world, with widespread access to the Internet and online services. Globally, it is estimated that one in every three children uses the Internet, which means that a significant portion of online users are under the age of 18. For many young people, the digital space serves multiple purposes—it is a source of education, entertainment, skill development, and a platform for building social connections and personal identity.

At the same time, this constant online presence brings serious concerns. The easy availability of digital content often exposes children to material that is not appropriate for their age, along with a range of online risks. Due to their stage of development, children are particularly vulnerable to cyber predators and other harmful actors who may exploit their lack of awareness or maturity.

The situation became even more complex during the COVID-19 pandemic. With lockdowns and movement restrictions in place, digital platforms became essential, especially as schools shifted from traditional classrooms to online modes of teaching. Although this helped maintain educational continuity, it also made learning more impersonal, reduced face-to-face interaction, and left many children socially isolated within digital environments. As a result, increased screen time and online engagement exposed children to greater risks affecting their safety, emotional well-being, and mental health. Reflecting this trend, official data from the National Crime Records Bureau reported a sharp 32% increase in cybercrimes against children between 2021 and 2022.

In the digital age, children face a range of emerging challenges such as excessive screen dependence, cyberbullying, and exposure to inappropriate or harmful content, including the growing circulation of

¹ Dr. Naveen Kumar, Protecting Child Rights in the Digital Era: Legal Challenges, Cyber Risks, and the Indian Regulatory Response, 3 INFINITE, 128, 129 (2026).

² *Ibid*

Child Sexual Abuse Material (CSAM). Online spaces like social media platforms, chat forums, and multiplayer games can also pose significant risks to their safety and privacy. A major concern is that many parents and guardians do not yet have the necessary digital awareness or skills to fully understand these threats or guide their children effectively, which can leave young users more exposed to emotional and psychological harm.

At the same time, the rapid spread of smart phones, tablets, and personal computers has made internet access almost universal among children. As a result, they are going online at increasingly younger ages and spending more time in digital environments, often without adequate supervision or safeguards.³

CONSTITUTIONAL PROVISIONS FOR CHILD PROTECTION

The constitutional framework of India provides a strong foundation for safeguarding children, and its principles can be meaningfully interpreted to address the complexities of the digital age.

Article 21: Right to Life and Dignity

Article 21 guarantees the right to life and personal liberty, which has been expansively interpreted to include the right to live with dignity, privacy, and security. For children, this extends beyond mere survival to encompass their emotional, psychological, and developmental well-being. Courts have increasingly acknowledged that online harms—such as cyber exploitation, grooming, and the circulation of child sexual abuse material—directly infringe upon a child's dignity and safety. Therefore, digital abuse falls squarely within the protective scope of Article 21.⁴

Article 19(1)(a): Freedom of Speech and Expression

Article 19(1)(a) guarantees the fundamental right to freedom of speech and expression, which includes the right to access information and express oneself through digital platforms. For children, this right is crucial in enabling participation in online education, communication, and creative expression. However, this freedom is not absolute and is subject to reasonable restrictions under Article 19(2) in the interests of decency, morality, and the protection of others. In the context of child rights, this provision justifies regulatory measures aimed at restricting harmful or inappropriate content online, thereby striking a balance between freedom of expression and the need to protect children from digital harms.⁵

Article 15(3): Special Provisions for Children

Article 15(3) empowers the State to make special provisions for women and children, thereby enabling targeted legal and policy interventions for their welfare. This provision forms the constitutional basis for child-specific legislation such as the Protection of Children from Sexual Offences Act, 2012 (POCSO Act), which addresses sexual abuse in both physical and digital contexts. It reflects the State's obligation to provide enhanced protection to children in recognition of their vulnerability.⁶

Article 39(e) and (f): Directive Principles of State Policy

Articles 39(e) and (f), as part of the Directive Principles of State Policy, impose a duty on the State to ensure that children are protected from abuse and are provided opportunities for healthy development in conditions of dignity and freedom. Although these provisions are non-justiciable, they serve as guiding principles for lawmaking and governance. In the digital era, they underscore the need for comprehensive

³ Sadhna Singh, Online Safety for Children: Protecting the next generation from harm <https://www.niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf>

⁴ INDIA CONST. art. 21.

⁵ INDIA CONST. art. 19, cls. (1)(a), (2).

⁶ INDIA CONST. art. 15, cl. 3; Protection of Children from Sexual Offences Act, No. 32 of 2012, INDIA CODE (2012).

measures to safeguard children from online exploitation and to foster a safe digital environment conducive to their overall development.⁷

LEGAL FRAMEWORK AGAINST ONLINE CHILD SEXUAL ABUSE IN INDIA

India has developed a multi-layered legal framework to combat online child sexual abuse, combining child-specific legislation with broader cyber and welfare laws. These statutes collectively aim to prevent exploitation, criminalize offenders, and provide protection and rehabilitation for victims in an increasingly digital environment.

Protection of Children from Sexual Offences (POCSO) Act, 2012

The Protection of Children from Sexual Offences Act, 2012 is the primary legislation addressing child sexual abuse in India. It adopts a comprehensive approach by criminalizing a wide range of offences, including sexual assault, harassment, and pornography involving children. Importantly, the Act extends to digital spaces by penalizing the creation, possession, distribution, and transmission of Child Sexual Exploitative and Abuse Material (CSEAM). It also incorporates child-friendly procedures for reporting, recording evidence, and conducting trials, ensuring that victims are not subjected to further trauma during the legal process. The gender-neutral nature of the Act further strengthens its scope, making it applicable to all children regardless of gender.

Section 11 of the Act defines Sexual harassment of Children while 12 prescribes punishment for such harassment.⁸ Section 13 and 14 address the use of children for pornographic purposes covering media, print or electronic form to produce, distribute or create such material and provide punishment for employing children in such activities.⁹ Section 15 further criminalizes the storage or possession of pornographic material involving Children.¹⁰ Section 16 makes aiding or abetting the commission of these offences punishable under the law.¹¹

The act also recognizes the responsibility of institutions and intermediaries in preventing child exploitation. Section 20 imposes a mandatory duty on media personnel, studios and photographic facilities to report sexually exploitative, pornographic or obscene material involving children to the special juvenile Police Unit or local police.¹² Failure to comply with the obligation is punishable under Section 21.¹³

To strengthen the law in response to technological advancements and emerging forms of exploitation, the 2019 amendment to the POCSO Act expanded its scope by enhancing punishment and introducing a statutory definition of Child pornographic under Section 2(da).¹⁴ This provision defines child pornography as any visual depiction of sexually explicit conduct involving child, including photographs, videos, digital or computer-generated images, or modified images that appear to depict a child.¹⁵

The Information Technology Act, 2000

The Information Technology Act, 2000—along with the rules on Reasonable Security Practices and Pr-

⁷ INDIA CONST. art. 39, cls. (e)–(f).

⁸ The Protection of Children from Sexual Offences Act, 2012 No. 32, Ss 11-12 Acts of Parliament, 2012(India).

⁹ The Protection of Children from Sexual Offences Act, 2012 No. 32, Ss 13-14 Acts of Parliament, 2012(India).

¹⁰ The Protection of Children from Sexual Offences Act, 2012 No. 32, S 15 Acts of Parliament, 2012(India).

¹¹ The Protection of Children from Sexual Offences Act, 2012 No. 32, S 16 Acts of Parliament, 2012(India).

¹² The Protection of Children from Sexual Offences Act, 2012 No. 32, S 20 Acts of Parliament, 2012(India).

¹³ The Protection of Children from Sexual Offences Act, 2012 No. 32, S 21 Acts of Parliament, 2012(India).

¹⁴ The Protection of Children from Sexual Offences Act, 2019 No. 25, Acts of Parliament, 2019(India).

¹⁵ The Protection of Children from Sexual Offences Act, 2012 No. 32, S 2(da), Acts of Parliament, 2012(India).

cedures and Sensitive Personal Information, which came into effect on 17 October—served as India’s main law for personal data protection. Following the amendments made in 2008, several provisions related to data protection and privacy were introduced and strengthened.

Section 66E of the Information Technology Act, 2000¹⁶ provides that if any person intentionally or knowingly captures, publishes or transmits an image of a person private area without consent, violates privacy and are liable. Since children can be vulnerable to the unauthorized sharing of their data or sensitive information, this provision offers a means of protection and remedy.

Section 67B of the Information Technology Act, prohibits the publishing, transmission, creation or sharing of any material that depicts children engaged in sexually explicit act or child abuse. This provision safeguards children against exploitation in the online environment.

Section 72 penalizes any person who while exercising power under the Act or in possession of the personal data disclose such information without the consent of the person. Prevents the unauthorized disclosure of personal information and ensures that children’s data is safeguarded by organizations.¹⁷

Section 43A of the makes it mandatory for the organisations handling sensitive personal data or information must implement reasonable security practices to protect it if they fail to do so they can be held liable.¹⁸ Although the IT Act includes provisions related to privacy, it lacks detailed measures specifically addressing children’s privacy, such as requirements for parental consent and age verification.

The Indian Digital Personal Data Protection Act, 2023

The Indian Digital Personal Data Protection Act, 2023, which came into effect on August 11, 2023, marks a significant step forward in safeguarding personal data in India, particularly for children. Recognizing that children are more vulnerable to privacy risks, the Act introduces specific provisions to ensure their data is handled with greater care. Children’s personal data includes details such as their name, address, date of birth, biometric information, educational records, and any other data that reveals insights into their activities.

According to Section 2(f) of the Digital Personal Data Protection Act 2023, a child is defined as “an individual who has not completed the age of eighteen” (18 years)

Section 9 of the Act deals with safeguarding children’s privacy. It places an obligation on the data fiduciary to obtain parental consent for age verification, but it does not specify any particular method for securing such consent.¹⁹

Section 9(2) of the Act prohibits data fiduciaries from processing children’s personal data in ways that could harm their well-being. This includes potential physical, emotional, or mental harm, requiring fiduciaries to adopt child-sensitive practices. Section 9(3) further restricts fiduciaries from engaging in activities such as tracking, behavioral monitoring, or targeted advertising directed at children. These practices are considered exploitative and capable of influencing children in ways that increase risks to their well-being. Overall, the Act emphasizes the need for data fiduciaries to prioritize ethical handling of children’s data.

Section 10 of the Act states that data fiduciaries are responsible for processing children’s personal data only for lawful purposes and in a manner consistent with the purpose for which the data was originally

¹⁶ The Information Technology Act, 2000, No. 21 of 2000, S 66E, Acts of Parliament, 2000 (India).

¹⁷ The Information Technology Act, 2000, No. 21 of 2000, S 67B, Acts of Parliament, 2000 (India).

¹⁸ The Information Technology Act, 2000, No. 21 of 2000, S 43, Acts of Parliament, 2000 (India).

¹⁹ Digital Personal Data Protection Act, No. 22 of 2023, S 9, India Code (2023).

collected. Section 10 empowers the Central Government to designate certain entities as Significant Data Fiduciaries (SDFs) based on factors such as the volume and sensitivity of personal data processed and the risk to the rights of Data Principals. SDFs are required to conduct periodic Data Protection Impact Assessments (DPIAs), which assess and manage risks to the rights of Data Principals.²⁰ In the context of children's data, these assessments must evaluate potential risks to children's privacy and well-being and ensure that data processing activities remain safe.

Section 18 outlines penalties for violations and non-compliance with the Act, including instances where children's data is processed without obtaining parental consent. Such breaches can lead to fines and other penalties.²¹

However, the Digital Personal Data Protection Act does not comprehensively address the protection of children's personal data. Multiple stakeholders are involved in the collection and use of such data, increasing the risk of misuse. For instance, social media platforms may fail to adequately safeguard children's personal information, which can then be exploited in ways that may harm them.

ROLE OF JUDICIARY IN ONLINE CHILD SAFETY

In response to the increasing nature of online abuse, Indian courts have expanded the scope of Child protection laws to address digital exploitation, cyber abuse, and the responsibilities of online platform. Recent judicial pronouncements reflect a more proactive and child-centric approach, reinforcing that Children's safety, dignity and well-being must remain protected even in virtual spaces.

In the case of **Just Rights for Children Alliance Vs. S. Harish**²², the Supreme Court strengthened India's legal response to Child Sexual Exploitative and Abuse Material(CSEAM) by clarifying that the possession, storage, consumption, and transmission of such material constitutes punishable offences. The court broadened the concept of constructive possession, ensuring that individuals exercising digital control over exploitative content may also be held liable. Moreover, the judgment also emphasized intermediary accountability, holding that online platform cannot claim immunity under section 79 of Information Technology Act unless they actively remove such material and comply with reporting obligations under the POCSO framework.

In **Kamlesh Devi Vs. State(NCT of Delhi)& Anr.**²³, the Delhi High Court, while addressing concerns relating to child safety in digital environments, highlighted the urgent need for awareness regarding "virtual touch" alongside traditional concept of good touch and bad touch. The court recognized that children today face not only physical but also online vulnerabilities, and stressed the importance of incorporating digital safety education into child protection strategies. This reflects a progressive judicial understanding of emerging forms of abuse in technologically mediated spaces.

CONCLUSION, RECOMMENDATIONS AND WAY FORWARD

CONCLUSION

The rapid integration of digital technologies into children's lives has fundamentally changed the nature of risks they face, shifting many threats from physical spaces to complex and often invisible online environments. While India's constitutional framework and existing legal provisions—such as the

²⁰ Digital Personal Data Protection Act, No. 22 of 2023, S 10, India Code (2023).

²¹ Digital Personal Data Protection Act, No. 22 of 2023, S 18, India Code (2023).

²² Just Rights for Children Alliance Vs. S. Harish, 2024 INSC 716(India).

²³ Kamlesh Devi v. State (NCT of Delhi) & Anr., Bail Appln. No. 216/2024.

POCSO Act, the Information Technology Act, and the Digital Personal Data Protection Act, 2023—provide an important foundation for child protection, they are not fully equipped to address the dynamic and evolving nature of digital harm.

The law continues to operate largely within traditional understandings of abuse, whereas online risks such as cyber grooming, algorithmic targeting, data exploitation, and anonymous offenders demand more adaptive and technology-sensitive responses. Although recent judicial interventions show a progressive shift toward recognizing digital harms, significant gaps remain in enforcement, accountability, and preventive mechanisms.

Ultimately, protecting children in the digital age is not only a legal challenge but also a societal responsibility. It requires a careful balance between enabling children to benefit from digital opportunities and ensuring that their dignity, privacy, and safety are not compromised. A more child-centric and future-oriented approach is essential to ensure that legal protections remain meaningful in an increasingly digital world.

RECOMMENDATIONS AND WAY FORWARD

To address the growing challenges of online child safety, a multi-dimensional approach is necessary—one that combines legal reform, institutional accountability, technological safeguards, and social awareness.

First, there is a need to strengthen the existing legal framework by making it more specific to children's digital rights. Laws should clearly define standards for age verification, parental consent, and data minimization, particularly under the Digital Personal Data Protection Act. Clearer guidelines will reduce ambiguity and improve compliance among data fiduciaries and digital platforms.

Second, greater accountability must be imposed on intermediaries and social media platforms. These entities should not only act as passive hosts but take proactive steps to detect, report, and remove harmful content involving children. This includes investing in safer platform design, stronger content moderation systems, and transparent reporting mechanisms.

Third, digital literacy and awareness must be prioritized at all levels. Parents, teachers, and children themselves need to be educated about online risks, privacy protection, and responsible digital behavior. Schools should incorporate digital safety education into their curriculum, helping children understand both their rights and the potential dangers of online spaces.

Fourth, law enforcement agencies must be better equipped to handle cybercrimes involving children. This includes specialized training, improved technological resources, and stronger coordination between national and international agencies, given the borderless nature of digital offences.

Fifth, there is a need to adopt a child rights-based approach in digital governance. Children should not be viewed merely as passive recipients of protection but as individuals with evolving capacities and rights. Policies must reflect their best interests while also respecting their autonomy and participation in the digital world.

Finally, collaboration between government bodies, private sector entities, civil society, and international organizations is essential. Addressing online child safety is a shared responsibility, and only a coordinated effort can ensure effective and sustainable protection.

In moving forward, India must aim to create a digital ecosystem that is not only innovative and inclusive but also safe and respectful of children's rights. A balanced, forward-looking approach—grounded in constitutional values—will be key to achieving this goal.

REFERENCES

1. Roy, J. S. (2021). Instrument to protect rights of children: Revisiting the impact of legislative and societal policies for development and protection of children. *Journal of Emerging Technologies and Innovative Research*, 8, 748–752.
2. Dr. Naveen Kumar, Protecting Child Rights in the Digital Era: Legal Challenges, Cyber Risks, and the Indian Regulatory Response, 3 INFINITE, 128, 129 (2026).
3. Sadhna Singh, Online Safety for Children: Protecting the next generation from harm <https://www.niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf>.

ACTS/CONSTITUTION

1. The Constitution of India, 1950.
2. The Protection of Children from Sexual Offences Act, 2012.
3. The Juvenile Justice (Care and Protection of Children) Act, 2015.
4. The Information Technology Act, 2000.
5. Digital Personal Data Protection Act, 2023