

Indian Constitution's Resilience in Protecting Children from AI-based Social Media Harms

Nanthika Venkatesan*

* LLM Student from School of Excellence in Law, TNDALU, Chennai

Research Article History

Received: 21-Apr-2026
Revised: 15-Sep-2026
Accepted: 16-Sep-2026
Published: 01-Oct-2026

Keywords

AI
Children
Constitutional resilience

Abstract

This paper examines, Indian Constitution's resilience in safeguarding children's rights from digital vulnerabilities such as surveillance, behavioural manipulation, and data exploitation. Although existing legal frameworks, including the Information Technology Act, the Protection of Children from Sexual Offences Act, and the Digital Personal Data Protection Act, offer a basic level of protection to children in digital platforms, they are currently fragmented and struggling to keep pace with the rapid evolution of AI technology. This paper critically examines whether the Indian Constitution is resilient in protecting children from AI-based digital vulnerabilities. It employs doctrinal and comparative methodology for analysis and identifies challenges such as systemic bias in India's digital governance system. The paper argues that India requires child-centric, AI-based legal framework that integrates constitutional rights, particularly the right to dignity, privacy, and equality, into our digital governance. It also recommends harmonizing Indian law with global best practices while adapting them to India's socio-legal context.

Corresponding Author:

Nanthika Venkatesan*

LLM Student from School of Excellence in Law, TNDALU, Chennai

This article is under the [CC BY-NC-ND](#) licenses
Copyright @ Journal of Law and Legal Research
Development, available at www.jllrd.com



1. INTRODUCTION

The new dilemma in India is that AI-based social media is both directly and indirectly digitizing childhood and benefiting from it at the cost of its childhood. The gravity of this threat is illustrated in the Netflix documentary *The Social Dilemma* though these platforms offer benefits, the uncensored nature of many social media environments puts minors at the disadvantage. These platforms which have built-in algorithms are designed to maximize engagement, exposing minors to harmful content, and thereby facilitating cyberbullying, online grooming and exploitation. (Mulaah et al., 2025). This concern is supported by studies, which has identified the "visible adjustment of content offerings", based on the user's behaviour in online sessions or social media usage patterns (Hilbert et al., n.d.). Other empirical evidence of AI-linked harm to Indian children shows that AI-driven social media algorithms amplify cyberbullying, unhealthy social comparison, sleep disruption, and anxiety among adolescents. The data of the study indicates that 44% of Indian children have experienced cyberbullying, 30% of adolescent's report feelings of inadequacy due to algorithmically curated comparisons, and 72% suffer sleep

disturbances linked to excessive, engagement-maximising platform design. (Dey, 2025). The presence of minors on the online platforms is both real and detectable by these platforms; however, there are no mechanisms in place to verify and block underage users. These rapid developments give rise to legal and social challenges, requiring legal and ethical policy responses that protects the children's well-being. (Gonzalez-Torres, 2025).

2. LITERATURE REVIEW

Though legislations like Information Technology Act 2000, the Protection of Children from Sexual Offences Act, 2012, and the Digital Personal Data Protection Act, 2023 exist, the academic papers consistently emphasis on the lack of enforcement and their inadequacy in overriding the effects of AI vulnerabilities (Kadian et al., 2025) (Aadhavan & -, 2024) (Mulaah et al., al, 2025) (Bharal et al., 2025) (AV. & -, 2024). Furthermore, algorithmic bias threatens fairness and equality, thereby undermining constitutional protections and ethical AI deployment (Sujith Dinkar, 2025) (AV. & 2024) (Hilbert et al., n.d.). As there exists fragmented policy coupled with uncoordinated stakeholders' position, the legal gap between

constitutional rights and social media regulation in safeguarding minors is readily apparent (Bharal et al., 2025). In this context, it’s pertinent to balance children’s digital rights with freedom of expression, privacy and equality.

3. OBJECTIVE OF THE PAPER

To address the policy gap identified above, this paper aims to integrate constitutional rights with AI governance principles, to frame child-centric policy. It applies doctrinal and comparative methodologies to analyse, firstly, the efficiency of existing Indian policies relating to protection of children from AI-related social media harms. Secondly, it seeks to compare and assess India’s legal mechanisms against international standards for protection child rights. Thirdly, to give suggestions on how to improve Indian digital policy to make it a safe environment for minors.

4. MEANING AND SCOPE OF THE TERM “MINORS” AND “SOCIAL MEDIA” IN INDIA.

Across Indian legislations, the definitions for *child and minor* are fairly consistent; however, Indian constitution has stipulated varied age brackets based on nature of rights involved. In context of digital platforms, the Digital Personal Data Protection (DPDP) Act, 2023 and The Information Technology Act, 2000 (IT Act) and The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 uniformly consider individuals below the

age of eighteen (18) to be minors, thereby entitling them to a more stringent legal protection. In India, the scope of *social media platform* is not defined under one umbrella term but is instead categorised under different heads based on their functions and scale of operations. Section 2(w) and 2(v) of the IT rules, 2021 - Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 – categories, digital platform as Social Media Intermediary (SMI) and Significant Social Media Intermediary (SSMI). Smaller regional, niche digital platforms fall under SMI whereas platforms with a specific number of registered users in India – as notified by Central government – like YouTube, Instagram, classified under SSMI. SSMI are subjected to higher level of due diligence than SMIs.

5. CONSTITUTION’S RESILIENCE

Although Indian Constitution does not explicitly refer to “digital platforms” or “Artificial Intelligence”, it is a living document, whose profound principles are capable of being applied to the new-era threats of AI. Through newer legislations, statutory amendments and evolving judicial interpretations, constitutional values continue to be applied to new-age challenges posed by AI-based digital spaces. This adaptive nature highlights versatility of our constitution to stand against the test of time, and renewing itself to protect rights of its people, particularly, children

Table 1: Constitutional Principle

Article	Constitutional Principle	Application against AI threats in protecting minors
Article 15(3)	Bestows on state to frame special provisions for welfare of children	This becomes the foundation for acts like <i>POCSO, DPDP, IT Act and Rules</i> regulating digital interactions <i>Sec 9 of DPDP</i> act elaborates on conditions under which personal data of children may be processed. It prohibits the Data Fiduciary – defined as “any entity that determines purpose and means of processing personal data” <i>under sec 2(i)</i> of DPDP act, 2023 - from processing child’s personal data without parental or legal guardian consent. Furthermore, <i>sec 9(3) of act</i> prohibits “tracking or behavioural monitoring of children or targeted advertising directed at children”
Article 19(2)	Freedom of speech and Expression with reasonable restrictions	This permits state to impose reasonable restrictions on freedom of speech in interest of public order, decency and morality. It enables state to interfere and block harmful digital contents like child pornography. In extension of this constitutional principle, <i>section 4(4) of IT rules, 2021</i> , mandates additional due diligence to SSMI to deploy tech-based automated tools – AI-based mechanisms – to identify and remove child sexual abuse material (CSAM)
Article 21	Right to Privacy embedded within Right to Life and Personal Liberty	This ensures children are protected against unauthorized digital surveillance, data breaches, and the misuse of their personal information The wide judicial review powers bestowed by constitution to Supreme Court and High Courts can play a vital role in enforcement of digital rights of children, while maintaining their safety. Henceforth, if AI tools violate privacy of children, courts can step-in immediately.
Article 39(f)	Directive Principle of State Policy (DPSP), mandates the state to provide opportunities to ensure development of children in healthy, free and dignified manner.	This stands as a base to the creation of policy guidelines that advises against <i>rabbit hole algorithms</i> , excessive screen time and digital addiction In alignment with constitutional values, National Commission for Protection of Child Rights (NCPCR), a statutory body, established on the principles of constitution and UN convention of Rights of the Child (UNCRC), has initiated AI-driven measure to combat child sexual abuse material (CSAM) (Thacker, 2025) It has even issues guidelines “Prevention of Bullying and Cyberbullying in Schools (2024 – 2025)”, acting as a manual for ensuring schools have safe environment through counselling, and reporting mechanisms. (NCPCR, 2024) Similarly, the <i>Indian Academy of Paediatrics Guidelines on Screen Time and Digital Wellness in Infants, Children and Adolescents</i> , provides evidence-based clinical guidelines on the ill-effects of prolonged screen times, and recommends measures such as: introducing “screen free zones”, prescribing daily time limit and parental supervision to overcome harms of digital media. (Gupta et al., 2021)

6. VISION OF OUR CONSTITUTION

The framers of constitution in 1950 might not have anticipated contemporary AI-related concerns such as algorithmic biases, or digital privacy but they have crafted a constitution that is resilient enough to tackle evolving challenges. For instance, the “golden triangle” of Article 14, 19 and 21 continues to serve as the modern tool for resolving modern challenges as seen in *Shreya Singhal v. Union of India*, (2015) and *Navtej Singh Johar v. Union of India*, (2018).

7. SHORTCOMINGS OF EXISTING LEGISLATIONS

As discussed above, existing legislations, rules and guidelines provide an elaborate framework for the protection of children in digital space. However, they have largely failed to build robust safeguards capable of addressing AI-driven algorithmic threats. The language used in current legislations are overly broad and lack technical specificity, thereby creating regulatory grey areas. Such ambiguity favours digital platforms deploying complex AI techs that do not fall within the traditional statutory terms like “automated” or “processing”. While child sexual abuse material (CSAM) and AI-generated deepfakes are criminalised under IT and POCSO Act, and AI-based tools are increasingly used to identify and block such materials, yet these measures are predominantly reactive rather than preventive. They penalise the harm after it has occurred rather than predicting algorithm design choices, thereby exploiting child’s vulnerabilities. Furthermore, policy instruments such as PRAGYATA Guidelines and the Indian Academy of Paediatrics (IAP) Guidelines etc., are merely advisory in nature and lack binding effect. This limits the effectiveness of the guidelines in ensuring compliance by digital platforms. (NCPCR, 2024) (Gupta et al., 2021). Although both legislations and media platforms stipulate minimum age limits, minors are often seen easily circumventing the existing protective measures and access the age-inappropriate content. At present, a reliable and effective age-gating tech-based system does not exist. Finally, while Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate social media intermediaries to use AI tools for reviewing content bias, there is no corresponding legal obligation regarding how recommendation algorithms prioritise content for children. In the absence of transparency, these intermediaries cannot be regulators who face challenge in identifying and proving “detrimental effect” as prohibited by the DPDP Act, 2023.

8. COMPARATIVE ANALYSES: ASSESSING INDIAN LAW AGAINST INTERNATIONAL STANDARDS

The India’s legal protections for children are aligned with global benchmarks such as UN Convention on the Rights of the Child (UNCRC) and the UK Age-Appropriate Design Code (AADC). Following are the examples where Indian law is in alignment with international standards: (*Convention on the Rights of the Child*, 1989) (*Information Commissioner's Office*, 2020) (Mootz and Blocker, n.d.) (UNICEF, 2026)

- The DPDP Act, 2023 mirrors *General comment No. 25 (2021) on children’s rights in relation to the digital environment*, in prohibiting behaviour tracking of children for commercial purposes.
- Similarly, the Preamble of the POCSO Act (2012) and the DPDP Act (2023) incorporates “best interests of

child” doctrine, which is the core principle under Article 3(1) of the UNCRC.

- Section 9(1) of DPDP Act, requires Data fiduciary to get parents or legal guardian’s consent prior to processing of child’s data and section 8(7)(a) – General obligations of data fiduciary – mandates erasing of personal data once the specified purpose is fulfilled. These norms are consistent with GDPR-level for “reasonable efforts” to verify age and consent.
- However, there still remains technical and legal gaps which challenges its resilience against international standards. Following are examples of shortcoming of Indian policy in comparison with international standards (*Convention on the Rights of the Child*, 1989) (*Information Commissioner's Office*, 2020) (Mootz and Blocker, n.d.) (UNICEF, 2026)
- UK AADC, emphasises on transparency in algorithmic functioning but Algorithm audits are not mandated by Indian digital law, which can help in evaluating the psychological impact of algorithm recommendation engines on children.
- Article 13 of UNCRC states “*The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds*”. *The blanket restriction of children under the age of 18 contradicts this art 13. Instead, India can incorporate age bracket-based restrictions.*

9. POLICY RECOMMENDATION

Though current Indian legal policy has foundational laws, integrating international best practices such as the UK Age-Appropriate Design Code (AADC) and the EU General Data Protection Regulation (GDPR) can help in addressing regulatory gaps. *The UK AADC* is an effective model for illustrating how a statutory law can force digital platforms to redesign AI for good. This code has interlinked 15 standards that target the mechanics of AI-driven platforms. Within 2 years of enforcement the code has analysed 91 changes across major platforms like TikTok, Instagram. For instance: It led to YouTube turning off “autoplay” by default for minors and TikTok implementing a “curfew” on push notifications to prevent addictive late-night usage. *The EU General Data Protection Regulation (GDPR)* serves as the global benchmark for data-driven AI regulation and provides the legal foundation for several of India’s current and proposed protections. The following recommendations to Indian law are made, after analysing international best practices: (*Convention on the Rights of the Child*, 1989) (*Information Commissioner's Office*, 2020) (Mootz and Blocker, n.d.) (UNICEF, 2026)

- High-privacy settings and safety filters must be mandated to be switched on by default for users who are children. For example, autoplay, infinite scroll and personalised recommendation engines to be disabled to prevent digital addiction in children
- Similar to periodic Data Protection Impact Assessments mandated under the DPDP Act, Algorithmic Audits must also be added to reduce user’s harm
- To implement safe and effective age-verification system, India can adapt age-assurance model where instead of verifying child’s age through sensitive data like official documents, AI-driven less intrusive tools can be used. For instance, facial analysis, where data must be deleted immediately after verification. As an extra precaution, AI tools must be audited for

algorithmic bias to ensure it does not discriminate children based on ethnicity or skin tone

- Laws should explicitly prohibit nudge techniques, AI designs that manipulate a child into spending more time online or providing more personal data
- Currently, IT Rules currently define "user harm" vaguely as any effect detrimental to a child, this must be refined to include specific AI-driven harms, such as automated promotion of content related to eating disorders and self-harm

10. CONCLUSION

Our Indian constitution displays a normative resilience in addressing AI-driven social media harms affecting children through its child-centric principles. However, constitutional

strength is not sufficient if enforceability of constitutional values is not carried out by the State. Henceforth, India must translate constitutional principle such as right to dignity, privacy into a child-centric AI governance system by harmonizing with international best practices.

Conflict of Interest

Conflict of interest declared none.

Funding

The review presented in the article did not receive any external financial support.

Acknowledgements

The authors express their gratitude to Dr. M.G.R. Educational and Research Institute for their valuable support.

11. REFERENCES

- Aadhavan, V. -, & -, K. T. (2024). Legal frameworks and policy gaps in protecting children from online exploitation in india: Challenges and solutions. *International Journal For Multidisciplinary Research*, 6 (6), . <https://doi.org/10.36948/ijfmr.2024.v06i06.31363>
- AV, S, & -, N.D. (2024). Legal challenges of artificial intelligence in india's cyber law framework: Examining data privacy and algorithmic accountability via a comparative global perspective. *International Journal For Multidisciplinary Research*, 6 (6), . <https://doi.org/10.36948/ijfmr.2024.v06i06.31347>
- Bharal, S., Sharma, R, Pandey, A, & Ahmed, S. (2025). Code, constitution and AI: Rethinking fundamental rights in the algorithmic era. <https://doi.org/10.71097/ijssat.v16.i3.8087>
- Chauhan, K. D. S., & Anupriya (2024). Darker patterns? Ai-generated persuasion and the regulatory void in indian law. *Journal of development policy and practicenull*, . <https://doi.org/10.1177/24551333241275752>
- Dey, D.N.C. (2025). Mental health of adolescents and youth in India: A critical analysis in the era of AI. *Global E-Journal of Social Scientific Research*, 1(2). doi:<https://doi.org/10.64706/egrvyh93>.
- Gonzalez-Torres, A. (2025). The impact of cybersecurity laws on child safety in the digital world. <https://doi.org/10.4018/979-8-3373-5132-2.ch006>
- Government of India (2023) *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, Legislation of India.
- Government of India (2000) *The Information Technology Act, 2000*, No. 21 of 2000, Legislation of India.
- Government of India (2021) *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, Notification No. G.S.R. 139(E) , Ministry of Electronics and Information Technology
- Government of India (2012) *The Protection of Children from Sexual Offences Act, 2012*, No. 32 of 2012, Legislation of India
- Government of India (1950) *The Constitution of India*, adopted 26 November 1949, in force 26 January 1950. New Delhi: Government of India.
- Gupta, P., Shah, D., Bedi, N., Galagali, P., Dalwai, S., Agrawal, S., John, J.J., Mahajan, V., Meena, P., Mittal, H.G., Narmada, S., Smilie, C., Ramanan, P.V., Evans, Y.N., Goel, S., Mehta, R., Mishra, S., Pemde, H., Basavaraja, G.V. and Parekh, B.J. (2021). Indian Academy of Pediatrics Guidelines on Screen Time and Digital Wellness in Infants, Children and Adolescents. *Indian Pediatrics*, [online] 59(3), pp.235–244. doi:<https://doi.org/10.1007/s13312-022-2477-6>.
- Hakimi, M., Sazish, B., Rastagari, M. A., & Shahidzay, K. (2024). Artificial intelligence for social media safety and security: A systematic literature review. <https://doi.org/10.32996/smjic.2023.1.1.2x>
- Hilbert, M., Cingel, D. P., Zhang, J., Vigil, S. L., Shawcroft, J., Xue, H., Thakur, A., & Shafiq, Z. (n.d.). #bigtech @minors: Social media algorithms personalize minors' content after a single session, but not for their protection. *Social Science Research Networknull*, . <https://doi.org/10.2139/ssrn.4674573>
- Information Commissioner's Office (2020) *Age appropriate design: a code of practice for online services*. Wilmslow: Information Commissioner's Office. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/> (Accessed: 5 February 2026).
- Kadian, S. P., Yadav, N., & Yadav, G. (2025). The impact of cybersecurity laws on the child safety in the digital world. <https://doi.org/10.4018/979-8-3373-5132-2.ch008>
- Mootz, J. and Blocker, K. (n.d.). *UK Age-Appropriate Design Code Impact Assessment Age-Appropriate Design Code Impact Assessment*. Available at: <https://www.childrenandscreens.org/wp-content/uploads/2024/03/Children-and-Screens-UK-AADC-Impact-Assessment.pdf>.
- Mulaah, C. J., Musa, A. Z., & Ibharim, N. S. B. (2025). Child protection and vulnerability in the context of uncensored social media. *International journal of social science and human research*, 08 (08), . <https://doi.org/10.47191/ijsshr/v8-i8-76>
- National Commission for Protection of Child Rights (NCPCR) (2024) *Preventing bullying and cyberbullying: Guidelines for schools*. New Delhi Available at: https://ncpcr.gov.in/uploads/1702548255657ad31ff39b4_preventing-bullying-and-cyberbullying-guidelines-for-schools.pdf .

- Rani, D. D. (2024). Protecting children from online grooming in india's increasingly digital post-covid-19 landscape: Leveraging technological solutions and ai-powered tools. *International journal of innovative research in computer science & technology*, . <https://doi.org/10.55524/ijircst.2024.12.3.8>
- *Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the on the free movement of such data, and repealing Directive 95/46/EC* (2016) *Official Journal of the European Union* L 119, pp. 1-88.
- Saldias, B. (2024). Designing child-centered content exposure and moderation. <https://doi.org/10.48550/arxiv.2406.08420>
- Sujith, M. P., & Dinkar, V. (2025). Algorithmic bias and the right to equality: Reimagining constitutional guarantees in the age of artificial intelligence. *I/RDO - journal of business management*, . <https://doi.org/10.53555/bm.v11i2.6403>
- Thacker, H. (2025c). *India Leverages AI to Tackle Online Child Sexual Abuse - The CSR Journal*. [online] The CSR Journal. Available at: <https://thecsrjournal.in/india-leverages-ai-to-tackle-online-child-sexual-abuse/> [Accessed 5 Feb. 2026].
- United Nations (1989) *Convention on the Rights of the Child*. Treaty Series, 1577, 3
- UN Human Rights Office of High Commissioner (2021), General comment No. 25 (2021) on children's rights in relation to the digital environment. Available at: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>
- UNICEF*. Digital Age Assurance, Age Verification Tools, and Children's Rights Online across the Globe: A Discussion Paper*. Available at: <https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf> (Accessed: 5 February 2026).
- Verma, V., Kumar, P. M. S., & Singhal, D. (2025). Safeguarding children's rights in the digital age. <https://doi.org/10.4018/979-8-3373-5132-2.ch011>