



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

SAFEGUARDING CHILDREN IN THE DIGITAL AGE: THE NEED FOR STRONGER LEGAL PROTECTION IN INDIA

Navni Krishna

1. Introduction

Rapid digitalisation has exposed children to an array of new online threats, transforming the internet from a space of learning and connection into one of potential exploitation and risk. Over the past decade, India's digital ecosystem has grown exponentially, with millions of children gaining access to the internet through affordable smartphones, online classes, and social media. While this connectivity has opened up remarkable opportunities for education, creativity, and empowerment, it has also given rise to a darker reality where predators exploit anonymity, advanced technologies, and weak cyber laws to target the most vulnerable users: children.

It has transformed how children engage with the online world, but it has also exposed them to new and alarming dangers. Emerging risks such as AI-generated child sexual abuse material (CSAM), increasingly sophisticated cyber-grooming tactics, and rising cases of online exploitation highlight the severity of the crisis. In India, the situation is intensified by a rapidly expanding digital population that is not matched by equally strong enforcement mechanisms or policy preparedness. As technology continues to evolve at high speed, it is essential that legal frameworks, institutional capacities, and enforcement systems evolve alongside it to ensure meaningful protection for children online. The challenge is not only technological, but it is moral, legal, as well as social.

2. Rise of Online Child Sexual Abuse and Grooming

The digital age offers unprecedented access to information and communication but also introduces severe hazards. One such hazard is Online Child Sexual Exploitation (OCSE), sometimes referred to as "cyber molestation." Online child abuse typically involves an adult who manipulates or coerces a child into exploitative activities. This exploitation manifests in numerous forms that include grooming, sextortion, cyberstalking, and the circulation of Child Sexual Abuse Material (CSAM). With social media, live-streaming apps, and online gaming spaces becoming central to children's lives, perpetrators have discovered new and largely unregulated platforms to carry out abuse.

A disturbing trend is the rise of online grooming, where offenders build trust with children through prolonged communication before exploiting them sexually or emotionally. Grooming can begin innocently through compliments, shared interests, or small favours, but often escalates into manipulation and threats once the offender gains psychological control. Social networking apps and

online games with chat features have become hotspots for such grooming, as anonymity makes tracing perpetrators extremely difficult.

According to a study conducted by the Environmental Influences on Child Health Outcomes (ECHO), children's total screen time increased dramatically during the early stages of the COVID-19 pandemic. Even after restrictions were lifted, their online exposure remained consistently high. This surge in screen time inadvertently increased children's vulnerability, as perpetrators used the digital shift to exploit emotional loneliness, digital naivety, and the lack of adult supervision. The anonymity of cyberspace, combined with encrypted communication platforms, allows offenders to act with impunity, often using fake profiles or hidden forums to contact minors. The result is an alarming increase in cyber-grooming and emotional manipulation leading to sexual exploitation.

The consequence of online child exploitation extend far beyond the immediate act of abuse and often result in long-term psychological and social harm. Victims may experience anxiety, depression, long-term esteem, post-traumatic stress disorder (PTSD), and feelings of shame and helplessness. In case involving AI-generated child sexual abuse material (CSAM) and deepfakes, the harm can be particularly severe because victims often face the fear manipulated images or videos maybe circulated indefinitely across digital platforms. The persistent nature of online content creates a sense of ongoing victimisation, even when the abuse is not physically perpetrated.

The social consequences are equally significant. Victims may encounter bullying, social isolation, reputational damage, and difficulties in forming trusting relationships. Children subjected to online grooming or exploitation frequently suffer disruptions in their educational and personal development, which can have lasting effects on their future well-being. Moreover, the rapid dissemination of digital content amplifies the scale of harm, making it difficult for victims to regain a sense of privacy and security. These psychological and social impacts demonstrate that online child exploitation is not merely a cybercrime issue but a serious violation of children's dignity, mental health as well as fundamental rights.

The profound and lasting harm suffered by victims underscores the importance of examining whether existing legal frameworks are adequately equipped to address emerging forms of digital exploitation.

3. Rise of AI-Generated Abuse and the Deepfake Challenge

Child Sexual Abuse Material (CSAM) traditionally referred to the filming, recording, or distribution of any visual representation depicting the sexual exploitation of minors. However, technological advances especially in Artificial Intelligence have completely reshaped this landscape. AI now enables the creation of "deepfakes" which are synthetic, hyper-realistic images or videos that falsely depict individuals, including children, in sexual contexts.

AI-generated CSAM poses a new and particularly insidious threat because it can be produced without involving a real child, making detection and prosecution far more difficult. Freely accessible deepfake generators and image-manipulation tools allow offenders to create lifelike abuse images from innocent photos found online, blurring the line between virtual and real-world exploitation. This technology has outpaced existing laws, leaving enforcement agencies with limited tools to address synthetic crimes.

The problem transcends law enforcement and moves into the realm of digital ethics. Tech developers, AI startups, and major platforms have a moral responsibility to anticipate the misuse of their innovations. Without strict safeguards, ethical review boards, and regulatory oversight, even well-

intentioned AI tools can be weaponised for exploitation. A culture of “responsible innovation” must therefore be embedded across the tech ecosystem prioritising child protection, transparency, and accountability. The advancement of AI must never come at the cost of children’s safety or dignity.

4. Gaps in Law and Enforcement Preparedness

India’s legal system has made significant strides in recognising and addressing child abuse, yet online crimes evolve faster than policy reform. Despite multiple statutory safeguards, major gaps persist in both law and enforcement preparedness.

The Protection of Children from Sexual Offences (POCSO) Act, 2012 criminalises the creation and distribution of child pornography under Sections 13 to 15. However, it does not explicitly criminalise *synthetic* or *AI-generated* imagery. Similarly, the Information Technology Act, 2000 prohibits publishing or transmitting sexually explicit material involving children (Section 67B), but this provision predates modern AI and deepfake technologies, leaving a loophole in the current digital landscape.

The Bharatiya Nyaya Sanhita (BNS), 2023, India’s new criminal code, also lacks a direct provision addressing online grooming which is a major and rising form of exploitation. While certain sections touch on offences against minors, the absence of digital-specific terminology limits its applicability to emerging threats.

Enforcement remains another weak link. Cyber-forensics units often lack advanced AI-based detection tools and specialised training, making it hard to trace or analyse synthetic imagery. Many police stations, especially in smaller towns and rural districts, remain overburdened and under-equipped to prioritise cyber cases. Moreover, crucial evidence is frequently stored on foreign servers, leading to jurisdictional delays and incomplete investigations. Coordination gaps between the National Commission for Protection of Child Rights (NCPCR), state cyber cells, and large digital platforms further weaken response systems. These gaps result in inconsistent reporting, delayed removal of harmful content, and fragmented action against online child exploitation.

5. Building a Safer Digital Future

To safeguard children in the digital era, India needs a multi-layered, comprehensive approach combining legal, institutional, technological, and educational reforms.

Legally, both the POCSO Act and the IT Act must be amended to explicitly recognise AI-generated CSAM and digital grooming as punishable offences. These updates will ensure that the law keeps pace with innovation. Institutional reforms must follow, including the establishment of dedicated Cyber Child Protection Units within police departments, equipped with AI-forensic capabilities and trained personnel to handle technologically complex investigations.

Collaboration with technology companies is equally critical. Platforms such as social media networks, messaging services, and cloud providers must assume proactive responsibility for detecting and reporting abusive content. Automated detection tools powered by AI can help identify grooming patterns, flag CSAM, and support early interventions.

At the community level, education and awareness play a transformative role. Schools should integrate digital literacy and online safety modules into their curricula, empowering children to recognise red flags and report suspicious behaviour. Parents, particularly in rural and semi-urban areas, must be

sensitised to the realities of online risks. Simple steps such as monitoring screen time, discussing safe internet use, and encouraging open communication can drastically reduce vulnerability.

Civil society, NGOs, and international agencies like UNICEF should continue to strengthen awareness campaigns, provide counselling support, and bridge the gap between victims, law enforcement, and the judiciary. Together, these stakeholders can build a more resilient digital environment.

6. Conclusion

Technology's immense power must always be balanced by strong safeguards that prioritise human welfare, especially that of children. Ensuring online safety is no longer optional—it is an urgent societal responsibility. India must strengthen its legal frameworks, equip law enforcement with modern tools, and foster a culture of digital awareness that reaches every home and school.

Safeguarding children in the digital age demands that our empathy, governance, and institutions evolve as rapidly as our technology does. Only through united, sustained effort can we ensure that the promise of digital progress does not come at the price of childhood itself.

As technology continues to reshape childhood experiences, India must ensure that its legal frameworks, institutions, and digital ecosystems evolve accordingly to safeguard every child's right to safety, dignity, and development in the online world.

REFERENCES

1. Anne Priya, What is an Online Child Sexual Exploitation & Abuse?, Children of India (Oct. 12, 2024), <https://childrenofindia.in/what-is-an-online-child-sexual-exploitation-abuse/>.
2. Bansi Patel, What is Child Sexual Abuse Material (CSAM)?, Bachpan India - Save the Innocence (Mar. 28, 2024), <https://bachpanindia.org/bachpan/what-is-child-sexual-abuse-material-csam/>.
3. Block CSAM, Centre for Child Protection Studies Kerala (CCSE Kerala), <https://ccse.kerala.gov.in/block-csam>.
4. Daryl Higgins, Deepfake AI Pornography is Becoming More Common – What Can Parents and Schools Do to Prevent It? (June 12, 2024), <https://theconversation.com/deepfake-ai-pornography-is-becoming-more-common-what-can-parents-and-schools-do-to-prevent-it-232248/>.
5. How Can We Keep Children Safe as AI Reshapes the Internet?, World Economic Forum (Mar. 20, 2026), <https://www.weforum.org/stories/2026/03/ai-children-digital-online-safety/>.
6. Monique Hedderson, How Has Children's Screen Time Changed During the COVID-19 Pandemic? (Feb. 15, 2023), <https://echochildren.org/wp-content/uploads/2023/02/How-has-childrens-screen-time-changed-during-the-COVID-19-pandemic.pdf>.
7. Programmes, India Child Protection, <https://www.childprotection.org.in/programmes-1>.
8. Real-Time Deepfakes Are Rewriting the Rules of Child Safety, World Economic Forum (Apr. 27, 2026), <https://www.weforum.org/stories/2026/04/ai-voice-deepfakes-child-safety/>.
9. Six Ways to Help End Online Child Sexual Exploitation and Abuse, Office of Strategy and Evidence Innocenti, <https://www.unicef.org/innocenti/six-ways-help-end-online-child-sexual-exploitation-and-abuse>.
10. United Nations Office on Drugs and Crime (UNODC), Global Programme on Cybercrime: Online Child Sexual Exploitation and Abuse, https://unodc.org/document/cybercrime/Study_on_the_Effects.pdf.