The Infinite
An International Peer Reviewed / Refereed Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 2 | February 2026
ISSN: 3048-9539 (Online)
Website: www.theinfinite.co.in

Protecting Child Rights in the Digital Era: Legal Challenges, Cyber Risks, and the Indian Regulatory Response

Dr. Naveen Kumar[1]

ARTICLE DETAILS

Research Paper

Keywords :

Child Rights, Digital Era, Cyber Risks, Online Exploitation, Indian Legal Framework, Data Protection, Child Safety

ABSTRACT

The rapid expansion of digital technologies has profoundly transformed the lives of children across the globe. In India, increased internet penetration, widespread use of smartphones, online education platforms, social media, and artificial intelligence–driven systems have created unprecedented opportunities for learning and development. Simultaneously, these developments have exposed children to complex cyber risks such as online sexual exploitation, cyberbullying, data misuse, digital surveillance, and algorithmic manipulation. The traditional understanding of child rights, which primarily focused on physical safety, education, and welfare, now requires reinterpretation in the context of the digital environment.

This research paper critically examines the protection of child rights in the digital era, with particular reference to India. It analyses the evolving nature of cyber risks faced by children, evaluates the adequacy of the existing legal and regulatory framework—including constitutional provisions, child protection laws, cyber laws, and data protection regimes—and identifies gaps in enforcement and policy coherence. The study also draws upon international legal standards and comparative practices to assess India's compliance with global child rights obligations. The paper argues that while India has made notable legislative efforts to safeguard children in cyberspace, significant challenges remain in implementation, awareness, technological

[1] B.Sc, M.A., LLM, NET, Ph.D.(Law)

preparedness, and child-centric digital governance. It concludes by emphasizing the need for a holistic, rights-based, and future-oriented regulatory approach that balances digital innovation with robust child protection mechanisms.

1. Introduction

The concept of child rights has traditionally been rooted in the protection of children from physical harm, neglect, exploitation, and abuse, while ensuring access to education, health, and social welfare. However, the digital revolution has fundamentally altered the environment in which children grow, learn, and interact. In contemporary India, children are among the most active users of digital technologies, engaging with online education platforms, social networking sites, gaming applications, and artificial intelligence–enabled services from an increasingly young age. While these digital tools offer immense benefits, they also introduce new and complex threats that challenge conventional child protection mechanisms.

The digital space has blurred the boundaries between the public and private spheres, making children vulnerable to forms of harm that are often invisible, transnational, and technologically sophisticated. Online sexual exploitation, cyber grooming, exposure to harmful content, cyberbullying, identity theft, and unauthorized data collection have emerged as serious threats to the dignity, privacy, and safety of children. Unlike traditional forms of abuse, cyber risks often occur beyond the physical reach of parents, teachers, and law enforcement agencies, thereby complicating detection and accountability.

In India, the constitutional vision of child welfare is reflected in various provisions emphasizing protection, development, and dignity. However, these principles were formulated in a pre-digital context and now require reinterpretation to address emerging technological realities. The challenge before the Indian legal system lies not only in extending existing child protection laws to cyberspace but also in developing new regulatory frameworks that are responsive to rapidly evolving digital technologies.

This paper seeks to explore how child rights can be effectively protected in the digital era, with a specific focus on the Indian regulatory response. It examines whether current laws are adequate to address cyber risks faced by children and evaluates the extent to which India's legal framework aligns with international child rights standards. The study adopts a doctrinal and analytical approach, relying on statutes, judicial pronouncements, policy documents, and scholarly literature.

2. Conceptual Framework: Child Rights in the Digital Context

2.1 Understanding Child Rights

Child rights are a subset of human rights that recognize the special needs, vulnerabilities, and developmental requirements of children. These rights encompass civil, political, economic, social, and cultural dimensions, including the right to survival, development, protection, and participation. The recognition of children as rights-holders, rather than passive recipients of welfare, marks a significant shift in legal and moral philosophy.

In the Indian context, child rights are derived from constitutional principles, statutory enactments, and international commitments. These rights are not static; they evolve in response to social, economic, and technological changes. The digital era has expanded the scope of child rights by introducing new dimensions such as the right to digital privacy, online safety, and access to information in a secure environment.

2.2 The Digital Environment and Children

The digital environment refers to online platforms, digital services, communication technologies, and data-driven systems that shape social interactions. For children, this environment serves as a space for education, entertainment, socialization, and self-expression. However, children's limited cognitive maturity, lack of digital literacy, and dependence on adults make them particularly vulnerable to exploitation and manipulation in cyberspace.

Unlike adults, children may not fully understand the long-term consequences of sharing personal information online or engaging with unknown individuals. Digital technologies often collect, process, and monetize children's data without their informed consent, raising serious concerns about privacy and autonomy. Thus, the digital environment necessitates a child-centric rights framework that prioritizes safety, dignity, and best interests.

2.3 Reinterpreting the 'Best Interests of the Child' Principle

The principle of the "best interests of the child" is central to child rights jurisprudence. In the digital era, this principle must be interpreted in a manner that balances children's right to access digital resources with the obligation to protect them from harm. Blanket restrictions on internet access may hinder educational and developmental opportunities, while unrestricted access may expose children to serious risks.

A nuanced approach is required, wherein regulatory frameworks ensure age-appropriate design, parental guidance, digital literacy, and accountability of online platforms. The best interests principle thus serves as a guiding norm for evaluating digital policies and laws affecting children.

3. International Legal Framework on Child Rights and Digital Protection

3.1 Global Recognition of Digital Child Rights

At the international level, the recognition of child rights in the digital environment has gained momentum over the past decade. International instruments emphasize the need to adapt child protection mechanisms to technological advancements. Children's rights to privacy, freedom of expression, and protection from exploitation are increasingly interpreted through a digital lens.

Global organizations and child rights bodies have highlighted that digital technologies should be designed and regulated in a manner that respects and promotes child rights. The concept of "digital citizenship" underscores the importance of empowering children with knowledge, skills, and protections necessary to navigate the online world safely.

3.2 Obligations of States in the Digital Era

States bear the primary responsibility for ensuring that children are protected from digital harms. This includes enacting appropriate legislation, regulating online service providers, promoting awareness, and strengthening enforcement mechanisms. International norms emphasize that child protection in cyberspace requires cooperation between governments, private entities, civil society, and families.

For developing countries like India, the challenge is compounded by rapid technological adoption, digital inequality, and limited regulatory capacity. Nevertheless, international standards provide a normative framework against which domestic laws can be evaluated and reformed.

4. Review of Literature

Scholarly discourse on child rights in the digital era has expanded significantly in recent years. Researchers have emphasized that digital technologies create both empowering and endangering conditions for children. Studies highlight the growing prevalence of online abuse and exploitation, particularly in countries with high internet penetration and weak enforcement mechanisms.

Legal scholars have critiqued the inadequacy of traditional child protection laws in addressing cyber harms. They argue that existing legal frameworks often focus on post-harm remedies rather than

preventive and systemic measures. The lack of child-specific data protection standards has been identified as a major gap in many jurisdictions, including India.

Comparative studies suggest that countries with comprehensive child-centric digital policies are better equipped to address online risks. Such policies typically integrate child rights principles into data protection laws, platform regulation, and digital education strategies. Indian scholarship has increasingly called for harmonization between child protection laws and cyber laws to ensure effective implementation.

Despite growing literature, there remains a need for integrated studies that examine constitutional principles, statutory frameworks, and regulatory practices in a holistic manner. This paper seeks to contribute to this gap by providing a comprehensive analysis of India's regulatory response to digital child rights challenges.

5. Cyber Risks Faced by Children in India

5.1 Online Sexual Exploitation and Abuse

One of the gravest threats faced by children in the digital environment is online sexual exploitation and abuse. The internet has facilitated the circulation of child sexual abuse material, online grooming, live-streamed abuse, and coercive sexual interactions. Perpetrators often exploit the anonymity and accessibility of digital platforms to target children, making detection and prevention difficult.

In India, the rapid growth of social media usage among minors has intensified the risk of grooming and exploitation. Children are frequently lured through gaming platforms, messaging applications, and social networking sites. The psychological impact of such abuse extends beyond immediate harm, affecting mental health, self-esteem, and social development.

5.2 Cyberbullying and Online Harassment

Cyberbullying has emerged as a pervasive issue affecting children and adolescents. Unlike traditional bullying, cyberbullying operates continuously, transcending physical boundaries and exposing victims to persistent harassment. The viral nature of online content amplifies humiliation and emotional distress.

Indian studies indicate that cyberbullying among school-going children often remains underreported due to fear of stigma, lack of awareness, and inadequate institutional mechanisms. The absence of child-friendly complaint redressal systems further exacerbates the problem.

5.3 Data Privacy and Digital Surveillance

Children's data is routinely collected by online platforms through educational applications, social media services, and gaming interfaces. Personal information, behavioral patterns, and biometric data are often processed without meaningful consent. This raises serious concerns regarding privacy, profiling, and commercial exploitation.

Children lack the capacity to fully comprehend the implications of data sharing, making them particularly vulnerable to digital surveillance and misuse of personal information. The commodification of children's data poses long-term risks to autonomy and dignity.

5.4 Exposure to Harmful and Inappropriate Content

The digital ecosystem exposes children to violent, pornographic, extremist, and misleading content. Algorithm-driven platforms often prioritize engagement over safety, inadvertently promoting harmful material. Without effective content moderation and parental controls, children are likely to encounter age-inappropriate information that can adversely influence behavior and development.

6. Indian Legal and Regulatory Framework for Protection of Child Rights in the Digital Era

6.1 Constitutional Safeguards

The Constitution of India provides a foundational framework for child protection. Articles 14, 15(3), 21, 21A, 23, 24, 39(e) and 39(f) collectively emphasize equality, dignity, education, protection from exploitation, and welfare of children. The interpretation of Article 21 has expanded to include the right to privacy and human dignity, which are integral to digital child rights.

However, constitutional provisions do not explicitly address digital risks, necessitating statutory and regulatory intervention to operationalize these principles in cyberspace.

6.2 Protection of Children from Sexual Offences Act, 2012

The Protection of Children from Sexual Offences Act (POCSO) constitutes the primary legal instrument addressing sexual offences against children, including those committed through digital means. The Act criminalizes the use of children for pornographic purposes and recognizes electronic transmission as a mode of offence.

Despite its comprehensive nature, enforcement challenges persist. Jurisdictional complexities, lack of cyber forensic expertise, and delays in investigation undermine the effectiveness of the law in addressing online sexual exploitation.

6.3 Information Technology Act, 2000

The Information Technology Act provides a general framework for addressing cyber offences. Provisions relating to obscene content, child pornography, and intermediary liability are relevant to child protection. The Act empowers authorities to block harmful content and mandates intermediaries to exercise due diligence.

However, the Act was not originally designed with a child-centric approach. Its reactive orientation and limited emphasis on preventive safeguards reduce its effectiveness in addressing emerging cyber risks faced by children.

6.4 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act marks a significant development in India's data protection regime. The Act introduces special provisions for children's data, including requirements for parental consent and restrictions on data processing that may cause harm to children.

While the Act reflects progress towards recognizing children's privacy rights, concerns remain regarding implementation, enforcement capacity, and clarity of consent mechanisms. The absence of detailed child-specific compliance standards may limit its protective potential.

6.5 Juvenile Justice (Care and Protection of Children) Act, 2015

The Juvenile Justice Act adopts a rights-based approach to child protection, emphasizing care, rehabilitation, and best interests of the child. Although the Act does not directly regulate digital harms, its principles provide a normative foundation for addressing online abuse and exploitation.

Integration of digital safety considerations within child welfare institutions remains limited, highlighting the need for policy convergence.

7. Judicial Response to Digital Child Rights

Indian courts have played a proactive role in expanding the scope of child protection. Judicial pronouncements have emphasized the duty of the state to safeguard children from exploitation and ensure dignity in all circumstances. Courts have recognized the seriousness of online sexual offences and have issued directions for expeditious investigation and victim-centric procedures.

The recognition of the right to privacy as a fundamental right has indirect implications for children's digital rights. Judicial emphasis on constitutional morality and human dignity strengthens the normative basis for protecting children in cyberspace. However, jurisprudence specifically addressing digital child rights remains limited and fragmented.

8. Challenges in Protecting Child Rights in the Digital Era

Despite legislative and judicial efforts, multiple challenges hinder effective protection of child rights in the digital environment:

Fragmented Legal Framework: Lack of coordination between child protection laws, cyber laws, and data protection regimes creates regulatory gaps.

Enforcement Deficit: Limited technical expertise, inadequate infrastructure, and delayed investigations weaken law enforcement responses.

Low Awareness and Digital Literacy: Parents, teachers, and children often lack awareness of online risks and legal remedies.

Platform Accountability: Insufficient regulation of digital platforms and weak content moderation mechanisms undermine child safety.

Digital Divide: Socio-economic disparities affect access to safe digital resources and protective mechanisms.

9. Recommendations for Strengthening Digital Child Rights Protection

To ensure effective protection of child rights in the digital era, the following measures are recommended:

Adoption of a Child-Centric Digital Policy: A comprehensive national policy integrating child rights principles with digital governance.

Strengthening Legal Harmonization: Alignment of child protection laws with cyber and data protection frameworks.

Enhanced Platform Regulation: Mandatory child-safety-by-design standards for digital platforms.

Capacity Building: Specialized training for law enforcement, judiciary, and child welfare professionals.

Digital Literacy Programs: Awareness initiatives targeting children, parents, and educators.

Child-Friendly Complaint Mechanisms: Accessible and confidential reporting systems for online abuse.

International Cooperation: Cross-border collaboration to address transnational cyber crimes against children.

10. Conclusion

The digital era has redefined the landscape of child rights, presenting both unprecedented opportunities and complex challenges. In India, children's increasing engagement with digital technologies necessitates a re-examination of existing legal and regulatory frameworks. While constitutional principles, statutory enactments, and judicial interpretations provide a strong foundation, they are insufficient in isolation to address the multifaceted cyber risks faced by children.

This study highlights that effective protection of child rights in the digital environment requires a holistic, preventive, and rights-based approach. Legislative reforms must be complemented by robust enforcement, technological preparedness, and societal awareness. The integration of child rights into digital governance is not merely a legal necessity but a moral imperative essential for safeguarding the dignity, development, and future of children in an increasingly digital society.

References

Government of India. (2000). The Information Technology Act, 2000. Ministry of Electronics and Information Technology.

Government of India. (2012). The Protection of Children from Sexual Offences Act, 2012. Ministry of Law and Justice.

Government of India. (2015). The Juvenile Justice (Care and Protection of Children) Act, 2015. Ministry of Women and Child Development.

Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice.

United Nations. (1989). Convention on the Rights of the Child. United Nations General Assembly.

United Nations Committee on the Rights of the Child. (2021). General Comment No. 25 on children's rights in relation to the digital environment. United Nations.

UNICEF. (2017). Children in a digital world. United Nations Children's Fund.

UNICEF India. (2020). Child online protection in India: Policy and practice. UNICEF.

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. New Media & Society, 19(5), 657–670. https://doi.org/10.1177/1461444816686318

Livingstone, S., Stoilova, M., & Kelly, A. (2019). The benefits and risks of children's digital participation. London School of Economics.

Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2016). Global kids online research synthesis. UNICEF Office of Research.

Mehta, V., & Singh, P. (2021). Cyber crimes against children in India: Legal challenges and policy concerns. Indian Journal of Law and Justice, 12(2), 45–62.

Kumar, R. (2020). Child sexual abuse material and Indian cyber laws: A critical analysis. Journal of Victimology and Victim Justice, 3(1), 89–104.

Bhattacharjee, A. (2019). Child rights and digital privacy in India: Emerging legal issues. National Law University Law Review, 11(2), 233–250.

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

Supreme Court of India. (2018). Shafin Jahan v. Asokan K.M., (2018) 16 SCC 368.

OECD. (2021). Protecting children online: Policy responses and global trends. Organisation for Economic Co-operation and Development.

European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.

National Crime Records Bureau. (2022). Crime in India 2022. Ministry of Home Affairs, Government of India.

World Economic Forum. (2020). Advancing digital safety for children. World Economic Forum.