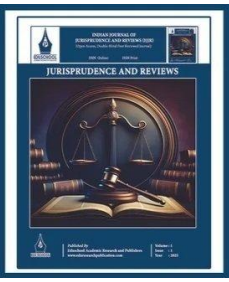
INDIAN JOURNAL OF JURISPRUDENCE AND REVIEWS (IJJR)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: 3139-177X



Cyberbullying and Child Safety Online in India: Evaluating the IT Rules and the Juvenile Justice Act

Lazar T A

Manager, St. Mary's U.P. School, Vendore, Amballur, Kerala, India

Article information

Received: 10th March 2026
Received in revised form: 14th April 2026
Accepted: 16th May 2026
Available online: 2nd June 2026

Volume: 2
Issue: 2
DOI: https://doi.org/10.63090/IJJR/3139.177X.0012

Abstract

The proliferation of digital technologies has exposed children to unprecedented risks of cyberbullying, necessitating robust legal frameworks for their protection. This paper critically examines the effectiveness of India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Juvenile Justice (Care and Protection of Children) Act, 2015, in addressing cyberbullying and ensuring child safety online. Through doctrinal analysis and evaluation of enforcement mechanisms, this study reveals significant gaps in implementation, coordination among stakeholders, and victim support systems. While the IT Rules impose due diligence obligations on intermediaries and the JJ Act provides rehabilitative frameworks, challenges persist in terms of definitional clarity, digital literacy, and swift redressal mechanisms. The paper argues for a comprehensive, child-centric approach integrating legal reforms, technological solutions, and educational interventions to create a safer digital environment for Indian children.

Keywords: - Cyberbullying, IT Rules, Information Technology Act, Online ethics, Digital Literacy

I. INTRODUCTION

The digital revolution has fundamentally transformed how children communicate, learn, and socialize. India, with over 700 million internet users and a median age of 28 years, has witnessed exponential growth in children's digital engagement (TRAI, 2023). However, this digital transformation has brought forth serious challenges, particularly cyberbullying, which has emerged as a critical threat to child safety and well-being. Cyberbullying encompasses various forms of online harassment, including threatening messages, non-consensual sharing of images, trolling, and exclusion from online groups, with potentially devastating psychological consequences for victims (Hinduja & Patchin, 2015).

Recognizing the urgency of this issue, India has enacted several legislative measures aimed at protecting children online. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter 'IT Rules, 2021'), represent a significant regulatory intervention imposing due diligence obligations on social media intermediaries. Simultaneously, the Juvenile Justice (Care and Protection of Children) Act, 2015 (hereinafter 'JJ Act, 2015'), provides a rehabilitative framework for children in conflict with law, including those involved in cybercrimes. Additionally, the Protection of Children from Sexual Offences Act, 2012 (POCSO Act), addresses online sexual exploitation, while relevant provisions of the Indian Penal Code, 1860, criminalize harassment and defamation.

Despite this multi-layered legal architecture, the effectiveness of these frameworks in curbing cyberbullying remains questionable. This paper critically examines whether India's current legal regime adequately addresses the complexities of cyberbullying and protects children's digital rights. The central research question guiding this inquiry is: To what extent do the IT Rules, 2021, and the JJ Act, 2015, effectively address cyberbullying and ensure comprehensive protection for children online? This analysis is crucial for identifying legislative gaps, implementation challenges, and potential reforms necessary for creating a safer digital environment for Indian children.

II. LEGAL AND THEORETICAL FRAMEWORK

2.1. Information Technology Rules, 2021

The IT Rules, 2021, promulgated under the Information Technology Act, 2000, establish a comprehensive regulatory framework for digital intermediaries. Rule 3(1)(b) mandates intermediaries to exercise due diligence, including removing or disabling access to unlawful content within specified timelines. Significantly, Rule 3(2)(b) requires platforms to enable users to identify and report content depicting children in sexually explicit acts or nudity. The Rules also establish a three-tier grievance redressal mechanism comprising Level I (Social Media Platform), Level II (Self-Regulatory Body), and Level III (Oversight Mechanism by the Central Government) (Ministry of Electronics and Information Technology, 2021).

For significant social media intermediaries (those with over 5 million registered users), additional obligations include appointing a Chief Compliance Officer, Nodal Contact Person, and Resident Grievance Officer, all of whom must be resident in India. These platforms must publish monthly compliance reports detailing complaints received and actions taken. However, the Rules do not explicitly define 'cyberbullying' or prescribe specific protocols for handling such complaints, creating ambiguity in enforcement (Dutta, 2023).

2.2. Juvenile Justice Act, 2015

The JJ Act, 2015, represents a paradigm shift from a punitive to a rehabilitative approach in dealing with children in conflict with law. Section 2(14) defines 'child in conflict with law' as any person below 18 years who is alleged to have committed an offense. The Act categorizes offenses as petty, serious, and heinous, with differentiated procedures for each category. Importantly, Section 8 establishes Juvenile Justice Boards (JJBs) with exclusive jurisdiction over children in conflict with law, ensuring a specialized, child-friendly adjudication process.

Section 15 emphasizes principles of best interest of the child, dignity and worth, and protection from harm throughout the juvenile justice process. The Act provides for various disposition options including counseling, community service, fine, probation, and institutional care in special homes. However, the JJ Act does not specifically address cybercrimes or cyberbullying, relying instead on general provisions applicable to all offenses committed by children (India Justice Report, 2023).

2.3. Complementary Legal Provisions

Several other legal provisions address aspects of cyberbullying. The POCSO Act, 2012, criminalizes sexual harassment of children through electronic means under Section 11. Sections 66C, 66D, and 67 of the IT Act, 2000, address identity theft, cheating, and publication of obscene material. The Indian Penal Code provisions on defamation (Sections 499-500), criminal intimidation (Section 506), and insult with intent to provoke breach of peace (Section 504) apply to cyberbullying conduct. The Digital Personal Data Protection Act, 2023, while recently enacted, provides enhanced protections for children's personal data online, though comprehensive implementation remains pending.

III. CRITICAL ANALYSIS OF EFFECTIVENESS

3.1. Definitional Ambiguities and Jurisdictional Gaps

A fundamental challenge lies in the absence of a statutory definition of 'cyberbullying' in Indian law. Neither the IT Rules, 2021, nor the JJ Act, 2015, explicitly define or categorize cyberbullying as a distinct offense. This definitional vacuum creates significant enforcement challenges, as investigating authorities and judicial forums must rely on analogous provisions that may not adequately capture the unique characteristics of cyberbullying. Unlike traditional bullying, cyberbullying operates continuously, involves potential anonymity, reaches wider audiences instantaneously, and creates permanent digital footprints (Kowalski et al., 2014). The existing legal framework fails to acknowledge these distinctive features, resulting in fragmented and inconsistent responses.

Furthermore, jurisdictional complexities arise when perpetrators and victims are located in different states or countries. While Section 75 of the IT Act, 2000, provides for extraterritorial jurisdiction, practical enforcement challenges persist in cross-border cases. The absence of bilateral or multilateral agreements for expedited digital evidence sharing hampers investigations, allowing perpetrators to exploit jurisdictional gaps.

3.2. Implementation Challenges of IT Rules, 2021

While the IT Rules impose stringent due diligence obligations on intermediaries, several implementation challenges undermine their effectiveness. First, the 24-hour timeline for removing unlawful content upon receiving court orders or government notifications (Rule 3(1)(d)) may be insufficient for addressing cyberbullying, which requires immediate intervention to prevent escalation and minimize harm. Studies indicate that delayed responses in cyberbullying cases exacerbate psychological trauma for victims (Patchin & Hinduja, 2017).

Second, the three-tier grievance redressal mechanism, while comprehensive on paper, lacks clarity regarding timelines and escalation procedures specifically for child safety concerns. The Rules do not mandate prioritization of complaints involving minors or establish child-specific complaint channels. Research suggests that general-purpose grievance mechanisms often fail to adequately address children's needs due to lack of specialized training and child-friendly procedures.

Third, the requirement for significant social media intermediaries to enable identification of first originators of information (Rule 4(2)) has sparked intense debates regarding privacy rights and encryption. While this provision aims to ensure accountability and traceability, implementation remains contentious and largely unenforced, particularly for end-to-end encrypted messaging platforms. This creates a regulatory stalemate where platforms claim technical impossibility while authorities insist on compliance, leaving children vulnerable in the interim (Internet Society, 2021).

3.3. Limitations of the Juvenile Justice Framework

The JJ Act, 2015, while progressive in its rehabilitative approach, faces several challenges in addressing cyberbullying effectively. First, the categorization of offenses as petty, serious, or heinous does not account for the psychological severity of cyberbullying, which may not fit traditional offense categories. A child engaging in severe, persistent cyberbullying causing significant psychological harm to the victim might be treated as committing a petty offense under the Act, resulting in disproportionately lenient dispositions that fail to deter such behavior or provide adequate justice to victims.

Second, Juvenile Justice Boards often lack specialized training and resources to handle cybercrimes. Most JJB members receive limited orientation on digital technologies, online behaviors, and the psychological dynamics of cyberbullying. This knowledge gap impedes effective assessment of culpability, appropriate disposition selection, and meaningful rehabilitation planning (Khurana & Chaturvedi, 2020).

Third, the Act's emphasis on institutional care and community-based rehabilitation may not adequately address the digital behavior modification necessary for child cyberbullying perpetrators. Traditional rehabilitation programs focus on offline behavioral interventions and may not include digital literacy, online ethics, or cyber-safety education components essential for preventing recidivism in cyberspace.

3.4. Victim Support and Redressal Mechanisms

Both frameworks exhibit significant gaps in victim support mechanisms. The IT Rules focus predominantly on intermediary obligations and content moderation, with minimal provisions for victim assistance, counseling, or rehabilitation. Similarly, while the JJ Act provides for Child Welfare Committees to address children in need of care and protection, cyberbullying victims often fall through the cracks of this system unless their cases involve severe abuse or neglect. The absence of dedicated cyberbullying helplines, specialized counseling services, and victim compensation mechanisms leaves affected children without adequate support during and after incidents. Furthermore, the stigma associated with reporting cyberbullying, combined with limited digital literacy among parents and educators, creates significant barriers to accessing existing redressal mechanisms.

IV. COMPARATIVE PERSPECTIVES AND BEST PRACTICES

International experiences offer valuable insights for strengthening India's legal framework. The European Union's General Data Protection Regulation (GDPR) provides enhanced protections for children's personal data, requiring parental consent for processing data of children under 16 years and mandating clear, child-friendly privacy notices (European Parliament, 2016). The United Kingdom's Online Safety Act, 2023, imposes duties of care on service providers to protect children from harmful content, including cyberbullying, with significant penalties for non-compliance. Australia's eSafety Commissioner serves as a dedicated regulatory authority with comprehensive powers to investigate cyberbullying complaints, order content removal, and coordinate national online safety initiatives (eSafety Commissioner, 2021).

These jurisdictions demonstrate that effective child protection online requires clear statutory definitions of cyberbullying, specialized regulatory authorities, swift content removal mechanisms, robust victim support systems, and mandatory digital literacy education. India can draw upon these models while adapting them to its unique socio-cultural context and constitutional framework, particularly the fundamental rights to freedom of speech and expression under Article 19(1)(a) and the right to privacy recognized in Justice K.S. Puttaswamy v. Union of India (2017).

V. RECOMMENDATIONS FOR LEGAL AND POLICY REFORM

Based on the foregoing analysis, this paper proposes several reforms to enhance the effectiveness of India's legal framework in addressing cyberbullying. First, India should enact comprehensive legislation specifically addressing cyberbullying, providing clear statutory definitions that encompass various forms of online harassment while distinguishing between age-appropriate peer conflicts and serious psychological harm. Such legislation should prescribe graduated responses based on severity, frequency, and impact of the bullying behavior.

Second, establishing a specialized Digital Safety Commissioner for Children, modeled after Australia's eSafety Commissioner, would provide dedicated oversight, investigation, and enforcement mechanisms. This authority should have powers to issue take-down notices, impose penalties on non-compliant intermediaries, coordinate with multiple stakeholders, and maintain a centralized database of cyberbullying incidents for policy development and research purposes.

Third, amendments to the IT Rules should mandate expedited response timelines specifically for complaints involving minors, require intermediaries to establish child-specific reporting mechanisms with child-friendly interfaces, and impose obligations to provide victim support services including counseling referrals and safety planning assistance. Platforms should be required to implement age-appropriate design features that minimize risks of cyberbullying, such as default privacy settings for children's accounts and proactive content moderation using artificial intelligence combined with human oversight.

Fourth, the JJ Act should be amended to recognize cyberbullying as a distinct category requiring specialized assessment and rehabilitation approaches. Juvenile Justice Boards should receive mandatory training in digital technologies, cyber psychology, and restorative justice practices suitable for online offenses. Rehabilitation programs should incorporate digital citizenship education, empathy development, and online behavioral interventions designed to prevent recidivism.

Fifth, India must prioritize comprehensive digital literacy education integrating cyber-safety, online ethics, and responsible digital citizenship into school curricula. Such education should target not only children but also parents, teachers, and community members who play crucial roles in preventing and responding to cyberbullying. Additionally, establishing school-based prevention programs employing evidence-based approaches such as the Olweus Bullying Prevention Program, adapted for the Indian context, can create supportive environments that reduce cyberbullying incidence (Olweus & Limber, 2010).

VI. CONCLUSION

This critical examination reveals that while India has established a multi-layered legal framework addressing various aspects of child safety online, significant gaps persist in effectively combating cyberbullying. The IT Rules, 2021, impose important obligations on intermediaries but lack child-specific provisions, expedited timelines for addressing bullying, and robust victim support mechanisms. The JJ Act, 2015, provides a rehabilitative framework for child offenders but fails to adequately address the unique characteristics of cybercrimes and cyberbullying perpetrators.

The effectiveness of these frameworks is further undermined by definitional ambiguities, implementation challenges, inadequate coordination among stakeholders, limited digital literacy, and insufficient resources for specialized training and victim support. Addressing cyberbullying requires not merely legal interventions but a comprehensive, multi-stakeholder approach integrating legal reforms, technological solutions, educational initiatives, and community engagement.

Moving forward, India must enact targeted legislation defining and criminalizing cyberbullying, establish specialized regulatory mechanisms for child protection online, mandate expedited response protocols, strengthen victim support systems, and prioritize digital literacy education. Only through such comprehensive reforms can India create a legal and social environment that effectively protects children from cyberbullying while respecting their rights to digital access, expression, and privacy. As technology continues to evolve, so too must our legal frameworks, ensuring that the law keeps pace with the digital realities shaping children's lives.

REFERENCES

Dutta, A. (2023). Evolving scope of intermediary liability in India. *International Review of Law, Computers & Technology, 37*(3), 328–348.

eSafety Commissioner. (2021). *Cyberbullying complaints system: Annual report 2020–21*. Australian Government.

European Parliament. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data*. Official Journal of the European Union.

Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Corwin Press.

India Justice Report. (2023). *Juvenile justice and children in conflict with the law: A study of capacity at the frontlines*. Tata Trusts.

Internet Society. (2021). *Internet impact brief: 2021 Indian intermediary guidelines and the internet experience in India*. Internet Society.

Juvenile Justice (Care and Protection of Children) Act, 2015, Act No. 2 of 2016 (India).

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

Khurana, A., & Chaturvedi, S. K. (2020). Juvenile justice system, juvenile mental health, and the role of mental health professionals: Challenges and opportunities. *Indian Journal of Psychological Medicine, 42*(4), 315–322.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073–1137.

Ministry of Electronics and Information Technology. (2021). *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Government of India.

Olweus, D., & Limber, S. P. (2010). Bullying in school: Evaluation and dissemination of the Olweus Bullying Prevention Program. *American Journal of Orthopsychiatry, 80*(1), 124–134.

Patchin, J. W., & Hinduja, S. (2017). Digital self-harm among adolescents. *Journal of Adolescent Health, 61*(6), 761–766.

Protection of Children from Sexual Offences Act, 2012, Act No. 32 of 2012 (India).

Telecom Regulatory Authority of India. (2023). *The Indian telecom services performance indicators: October–December 2022*. TRAI.