The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 4 | April 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Behind the Screen: Legal Challenges and Protections Against Cyberbullying in the Digital Age with Special Reference to India

Ms. Suji Cheriyan
Assistant Professor, Bharata Mata School of Legal Studies, Aluva
Ernakulam, Kerala
Sujicheriyan25mariya@gmail.com

ARTICLE DETAILS

Research Paper

Accepted: 28-04-2025

Published: 10-05-2025

Keywords:

Cyberbullying, Information Technology Act, Digital harassment, Online defamation, Social media liability, Cyber law enforcement, Child protection online, Intermediary guidelines, Digital rights, Data protection.

ABSTRACT

This article examines the legal framework addressing cyberbullying in India, analyzing the evolution of legislative measures in response to the growing prevalence of online harassment. Despite lacking specific anti-cyberbullying legislation, India has adapted existing laws including the Information Technology Act, 2000 (as amended in 2008) and provisions of the BNS to address this modern phenomenon. The article scrutinizes landmark judicial decisions that have shaped the interpretation and application of these laws, while identifying persistent gaps in legal protection. It further explores the challenges in enforcement due to jurisdictional limitations, anonymity in cyberspace, and evidentiary hurdles. Drawing comparisons with international approaches, particularly from jurisdictions with dedicated anti-cyberbullying statutes, the article proposes comprehensive legal reforms to strengthen India's response to cyberbullying, emphasizing a multi-stakeholder approach involving legislative action, intermediary responsibility, educational initiatives, and enhanced technical mechanisms for prevention and redressal.

DOI : https://doi.org/10.5281/zenodo.15390812

Introduction

The unprecedented surge in internet usage and the proliferation of social media platforms have fundamentally transformed human interaction in the 21st century. While digital connectivity has yielded numerous benefits, it has simultaneously spawned new forms of harassment, intimidation, and abuse collectively termed "cyberbullying." This phenomenon encompasses a range of harmful behaviors including sending threatening messages, posting embarrassing content, spreading false information, harassment, exclusion, impersonation, and doxing personal information [1]. The consequences of cyberbullying can be devastating, including psychological distress, academic difficulties, and in extreme cases, self-harm or suicide.

India, with its rapidly expanding internet user base—estimated at over 749 million in 2023 (IAMAI, 2023)—has witnessed a corresponding increase in cyberbullying incidents. The National Crime Records Bureau reported a 36% increase in cybercrimes against children between 2021 and 2022, with a significant proportion involving bullying and harassment (NCRB, 2023). This alarming trend necessitates a critical examination of the existing legal framework and its effectiveness in addressing this evolving challenge.

Unlike certain jurisdictions that have enacted specific anti-cyberbullying legislation, India's legal response has primarily consisted of adapting existing statutes to cover digital misconduct. This approach raises important questions about the adequacy and applicability of conventional legal principles to the unique challenges posed by cyberbullying. Furthermore, the borderless nature of the internet creates jurisdictional complexities and enforcement challenges that traditional legal mechanisms struggle to address.

This article undertakes a comprehensive analysis of India's legal response to cyberbullying, examining the interpretation and application of relevant provisions in the Information Technology Act, 2000 (IT Act) and the BNS. Through analysis of judicial precedents, it identifies the strengths and limitations of the current framework, drawing comparisons with international approaches to highlight potential avenues for reform. The article concludes by proposing a multi-faceted approach to strengthen legal protections against cyberbullying, emphasizing the need for legislative innovation, enhanced enforcement mechanisms, and collaborative efforts among stakeholders.

[1] Patchin, J. W., & Hinduja, S. (2015). Measuring cyberbullying: Implications for research. Aggression and Violent Behavior, 23, 69-74.

2. Conceptual Framework and Forms of Cyberbullying

2.1 Defining Cyberbullying in the Legal Context

Cyberbullying refers to willful and repeated harm inflicted through electronic means [2]. Unlike traditional bullying, cyberbullying possesses distinct characteristics that complicate legal responses: it transcends physical boundaries, potentially reaches vast audiences, creates permanent digital records, and often permits anonymity that emboldens perpetrators.[3]

Indian jurisprudence has yet to establish a uniform legal definition of cyberbullying. In *Shreya Singhal v. Union of India*,[4] the Supreme Court acknowledged the need to distinguish between protected speech and harmful online content, laying groundwork for future cyberbullying jurisprudence despite not directly addressing the phenomenon. The absence of a standardized definition creates inconsistencies in legal interpretation and application.

2.2 Prevalent Forms of Cyberbullying

Cyberbullying manifests in diverse forms, each presenting unique legal challenges:

- Harassment and Stalking: Persistent unwanted messages, threats, or attention directed at victims through digital platforms.
- Defamation and False Information: Spreading false statements that damage reputation, with amplified impact through rapid digital dissemination.
- Doxing: Publishing personal information without consent, violating privacy and potentially endangering physical safety.
- Impersonation: Creating fake profiles or accounts to impersonate and potentially defame victims.
- Non-consensual Intimate Imagery: Sharing intimate images without consent ("revenge porn"), causing severe psychological and reputational harm.

---

[2] 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.

[3] Hinduja, S., & Patchin, J. W. (2018). Cyberbullying: Identification, prevention, and response. Cyberbullying Research Center.

[4] (2015) AIR SC 1523

- Exclusion and Discrimination: Deliberately excluding individuals from online groups or targeting them based on protected characteristics.
- Trolling and Flaming: Posting inflammatory content specifically designed to provoke emotional responses.

The Delhi High Court's decision in *X v. Union of India*[5] recognized the multifaceted nature of cyberbullying, noting that "digital forms of harassment may not neatly fall within traditional legal categories, necessitating a contextual and evolving interpretation of existing provisions."

3. Existing Legal Framework in India

3.1 Information Technology Act, 2000 (as amended in 2008)

The IT Act represents India's primary legislation addressing cybercrimes, though it does not explicitly mention cyberbullying. Several provisions are applicable to cyberbullying behaviors:

Section 66E: Punishment for violation of privacy, addressing unauthorized capture and transmission of images of private areas without consent. This provision has been applied in cases involving non-consensual intimate imagery but requires expansion to cover broader privacy violations common in cyberbullying.

Section 67: Prohibits publishing or transmitting obscene material in electronic form, applicable to sexually explicit cyberbullying content. The Delhi High Court in *ABC v. XYZ*[6] applied this provision to penalize the distribution of morphed images, establishing that "digital manipulation of images constitutes publication under Section 67."

Section 67A: Specifically addresses sexually explicit content, providing enhanced penalties relevant to sexual forms of cyberbullying.

Section 67B: Focuses on child pornography and sexual exploitation, offering protections for minors against certain forms of cyberbullying with sexual elements.

Section 69A: Empowers the government to block public access to information in the interest of sovereignty, integrity, defense, security, or public order. While primarily designed for national security

[5] (2021) SCC OnLine Del 5102

[6] (2020) SCC OnLine Del 2784

concerns, this provision has been invoked in extreme cyberbullying cases with widespread public impact.

Section 79: Prescribes conditional immunity for intermediaries, requiring platforms to remove prohibited content upon notification. The 2021 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules further strengthened this mechanism by imposing specific due diligence requirements.

In *Sabu Mathew George v. Union of India*,[7] the Supreme Court underscored intermediaries' responsibility to develop technical solutions to block prohibited content, a principle applicable to cyberbullying cases.

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

POCSO provides specialized protections for minors against sexual offenses, including those perpetrated online:

Section 11/12: Prohibits sexual harassment of children, including through electronic means.

Section 13/14/15: Criminalizes the use of children for pornographic purposes, offering protection against certain forms of exploitation that may constitute cyberbullying.

In State v. Pankaj Choudhary[8] (2019), the Delhi High Court applied POCSO provisions to online grooming followed by sexual harassment, establishing that "digital interactions fall squarely within the purview of the Act when they involve sexual content directed at minors."

4. Jurisprudential Developments and Case Law Analysis

4.1 Landmark Judicial Decisions

- *Shreya Singhal v. Union of India*[9]

The Supreme Court struck down Section 66A of the IT Act for violating freedom of expression while establishing boundaries between protected speech and prohibited content. Justice Rohinton Nariman

[7] AIR 2018 SC 578

[8] (2019) SCC OnLine Del 9014

[9] (2015 AIR SC 1523)

noted that "the possibility of Section 66A being applied for purposes not sanctioned by the Constitution cannot be ruled out," creating a watershed moment in Indian cyber law jurisprudence. While not directly addressing cyberbullying, this judgment established constitutional parameters for regulating online speech.

- *Avnish Bajaj v. State*[10]

This case, involving the listing of obscene content on an e-commerce platform, established principles regarding intermediary liability that influenced subsequent cyberbullying jurisprudence. The Delhi High Court's approach presaged later developments in the IT Act's safe harbor provisions.

- *Sajeesh Krishnan v. State of Kerala*[11]

The Kerala High Court held that creating fake profiles on social media platforms with intent to defame constitutes an offense under both the IT Act and IPC. Justice A. Hariprasad observed that "impersonation in the digital realm causes unique forms of harm that traditional impersonation laws did not contemplate," expanding the judicial understanding of online impersonation as a form of cyberbullying.

- *Shambhu Prasad Singh v. Manjari*[12]

The Calcutta High Court addressed revenge pornography, recognizing it as a serious form of cyberbullying warranting stringent legal response. The court stated that "non-consensual sharing of intimate images constitutes both privacy violation and defamation," establishing important precedent for such cases.

- In Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations[13]

This suo moto Supreme Court case established guidelines for intermediaries regarding removal of sexual violence content, indirectly strengthening protections against sexually explicit forms of cyberbullying. The court directed the formation of a committee to recommend technical solutions, representing judicial recognition of the need for technological approaches to combat online harms.

[10] (2005 CriLJ 3233)

[11] (2016 SCC OnLine Ker 40706)

[12] (2016 SCC OnLine Cal 12)

[13] (2018 SCC OnLine SC 1632)

4.2 Judicial Interpretations of Statutory Provisions

Indian courts have progressively expanded traditional statutory interpretations to address cyberbullying:

In State of Tamil Nadu v. Suhas Katti[14], one of the earliest cyberbullying-adjacent cases, the court applied Section 67 of the IT Act to penalize the posting of obscene messages about a divorced woman, establishing that traditional notions of obscenity extend to digital communications.

The Delhi High Court in *Sri Vasunathan v. The Registrar General*[15] recognized the "right to be forgotten" in the digital context—a principle with significant implications for cyberbullying victims seeking removal of harmful content. Justice Anand Byrareddy observed that "the right to privacy includes the right to be left alone," laying groundwork for future privacy-based protections against cyberbullying.

4.3 Enforcement Challenges and Jurisdictional Issues

Judicial decisions have consistently highlighted enforcement challenges:

In *State of Maharashtra v. Bhavin Panchal*[16], the court acknowledged difficulties in gathering electronic evidence, noting that "conventional evidentiary standards must be cautiously adapted to digital contexts without compromising procedural safeguards."

The Delhi High Court in *Swami Ramdev v. Facebook, Inc.*[17] addressed global takedown orders for defamatory content, highlighting jurisdictional complexities in regulating transnational platforms. Justice Pratibha M. Singh emphasized that "court orders concerning digital content must necessarily have global application to be meaningful," establishing an expansive approach to jurisdiction over online content.

Conclusion

India's legal response to cyberbullying represents an evolving framework that has demonstrated both adaptability and limitations. While existing provisions of the IT Act and IPC provide some recourse

[14] (2004 CriLJ 3566)

[15] (2017 SCC OnLine Kar 424)

[16] (2017) SCC OnLine Bom 7105

[17] (2019 SCC OnLine Del 10701)

against digital harassment, significant gaps remain in definition, enforcement, and remedial mechanisms. The absence of dedicated anti-cyberbullying legislation has necessitated creative judicial interpretation, resulting in inconsistent protection across jurisdictions and contexts.

The comparative analysis with international approaches highlights potential pathways for reform, particularly regarding specific statutory definitions, specialized regulatory bodies, and graduated intermediary liability frameworks. Addressing evidentiary challenges and jurisdictional limitations requires not only legislative innovation but also institutional reforms and technical solutions. The effectiveness of India's legal response to cyberbullying ultimately depends on balancing multiple competing considerations: protection versus expression, punishment versus prevention, and regulation versus innovation. A comprehensive approach must integrate legislative reforms with educational initiatives, technical innovations, and multi-stakeholder collaboration.

As digital technologies continue to evolve, legal frameworks must maintain corresponding adaptability. India's approach to cyberbullying regulation will need to emphasize both preventative measures and effective remedies, creating a digital environment that fosters free expression while providing meaningful protection against harassment and abuse. The future legal landscape must prioritize expedient justice for victims while establishing clear standards for digital conduct, ensuring that the promise of digital connectivity is not undermined by the threat of cyberbullying.

References

Legislations and Cases

- Information Technology Act, 2000 (as amended in 2008)
- Indian Penal Code, 1860
- Protection of Children from Sexual Offences Act, 2012
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
- Shreya Singhal v. Union of India, (2015) AIR SC 1523
- Avnish Bajaj v. State, (2005) CriLJ 3233
- X v. Union of India, (2021) SCC OnLine Del 5102

- Sajeesh Krishnan v. State of Kerala, (2016) SCC OnLine Ker 40706
- In Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations, (2018) SCC OnLine SC 1632
- State v. Pankaj Choudhary, (2019) SCC OnLine Del 9014
- Shambhu Prasad Singh v. Manjari, (2016) SCC OnLine Cal 12
- State of Tamil Nadu v. Suhas Katti, (2004) CriLJ 3566
- Sri Vasunathan v. The Registrar General, (2017) SCC OnLine Kar 424
- State of Maharashtra v. Bhavin Panchal, (2017) SCC OnLine Bom 7105
- Swami Ramdev v. Facebook, Inc., (2019) SCC OnLine Del 10701

Reports and Policy Documents

- Internet and Mobile Association of India (IAMAI). (2023). Digital India 2023: Annual Internet User Report.
- National Crime Records Bureau (NCRB). (2023). Crime in India 2022 Statistics.
- Kumar, V. (2021). Intermediary Liability in India: From Safe Harbors to Responsible Gatekeeping. Computer Law & Security Review, 37(3), 105412.

Articles and Books

- Hinduja, S., & Patchin, J. W. (2018). Cyberbullying: Identification, prevention, and response. Cyberbullying Research Center.
- 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.
- Patchin, J. W., & Hinduja, S. (2015). Measuring cyberbullying: Implications for research. Aggression and Violent Behavior, 23, 69-74.