I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

Cyberbullying Laws in India: Current Challenges and Reforms

Rahul Dev Tyagi [1*], Prof. Dr. Om Dutt [2]
[1] Research Scholar, Maa Shakumbhari University, Saharanpur, Uttar Pradesh, India
[2] Head Department of Law, D.A.V. P.G. College, Muzaffarnagar, Uttar Pradesh, India

Corresponding Author: *Rahul Dev Tyagi

DOI: https://doi.org/10.5281/zenodo.17495517

Abstract

This paper examines the legal framework addressing cyberbullying in India, the challenges faced by victims, law enforcement, and intermediaries, and proposes reforms to enhance responses, making them more effective, victim-centric, and rights-respecting. The study covers statutory provisions under the Information Technology Act, 2000, and the Indian Penal Code (and proposed criminal law replacements), intermediary liability rules, landmark case law, enforcement realities, and comparative perspectives. It concludes with actionable recommendations for legislative, administrative, and technological reform.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 10-08-2025
- **Accepted:** 25-09-2025
- **Published:** 30-10-2025
- **IJCRM:**4(5); 2025: 523-526

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Tyagi RD, Dutt O. Cyberbullying Laws in India: Current Challenges and Reforms. Int J Contemp Res Multidiscip. 2025;4(5):523-526.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Cyberbullying, Cybercrime, POCSO, Harassment, Due diligence,

1. INTRODUCTION

The rapid spread of internet connectivity and social media has reshaped everyday communication in India. While these technologies have opened new opportunities for expression, education, and commerce, they have also made harassment, abuse, and bullying scalable and persistent. Cyberbullying — the targeted harassment of individuals using digital platforms — has significant mental-health, reputational, and physical-safety consequences. This paper analyses India's current legal and policy architecture to respond to cyberbullying, identifies its gaps, and proposes reforms to protect citizens better while safeguarding fundamental rights.

2. Definitions And Forms of Cyberbullying

Cyberbullying includes a wide range of harmful acts: repeated harassment via messages, image-based abuse (revenge pornography), doxxing (unauthorized disclosure of personal data), creation of fake profiles to humiliate or impersonate,

spreading false rumors, targeted trolling, threats, and coordinated abusive campaigns. The harm stems not only from the content itself but also from its circulation, permanence, and the difficulty of removal.

3. Legal Framework in India

3.1 Information Technology ACT, 2000

India's primary statute addressing digital behavior, the Information Technology Act, 2000 (IT Act), and its rules provide the statutory backdrop for cyber offences. Over time, judicial interpretation and rule-making have shaped how the IT Act is used to respond to online harassment. The IT Act originally contained provisions that allowed criminal charges for certain types of problematic online speech; however, overly broad provisions have been struck down, and other mechanisms — such as intermediary regulation — have become central to online content governance.

3.2 Bhartiya Nyaya Sanhita 2023 (Bns) And Related Provisions

Although the BNS 2023 predates the internet, several sections are routinely invoked in cyberbullying matters. These include provisions addressing stalking, criminal intimidation, insult to modesty, defamation, and transmission of obscene material. Law enforcement typically employs a combination of BNS 2023 offences and IT Act provisions (where applicable) to pursue perpetrators.

3.3 Other Statutes Affecting Online Harm (Pocso, Sexual Offences)

Image-based sexual abuse, child sexual abuse material (CSAM), and offences against children often fall under the Protection of Children from Sexual Offences (POCSO) Act and other sexual offenses provisions. The interaction between these laws and cyber-specific provisions requires careful handling to ensure evidence, forensic processes, and victim protections are consistent and robust.

3.4 Intermediary Liability and the It Intermediary Guidelines, 2021

Recognising the central role of intermediaries (platforms, hosting providers, social media companies), the government issued the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules impose due diligence obligations on intermediaries, including grievance redressal mechanisms, traceability requirements for certain messages, and timelines for removal of unlawful content upon receiving a valid order. The rules aimed to make platforms more accountable for online content, but they also raised concerns about privacy, overreach, and effects on speech.

4. Landmark Case Law

4.1 Shreya Singhal v. Union of India and the fate of Section 66A

In a landmark judgment, the Supreme Court struck down Section 66A of the IT Act in 2015 for being vague and overbroad, thereby curtailing the government's ability to arrest or prosecute individuals for vaguely defined online "offensive" speech. The decision reaffirmed constitutional protections for free speech and emphasised the need for narrowly tailored laws to address specific harms.

4.2 Subsequent judicial developments

Post-Shreya Singhal, courts have continued to grapple with balancing rights and harms — for instance, by upholding the validity of targeted takedown orders, interpreting intermediary obligations, and clarifying when criminal provisions under the IPC apply to online harms. Judicial oversight remains an essential check where administrative or platform processes risk overreach.

5. Enforcement and Practical Challenges

5.1 Identification, evidence, and anonymity

A primary challenge is identifying anonymous perpetrators. Digital forensics can sometimes trace IP addresses, device identifiers, or platform account metadata, but this depends on cooperation from intermediaries and lawful orders. Even when identification is possible, preserving evidence (message logs, screenshots, metadata) in admissible formats remains a technical and procedural challenge.

5.2 Capacity and training of law enforcement

Many police units lack specialised technical skills to investigate cyber offences properly. This manifests in delayed or inadequate investigations, improper handling of digital evidence, and occasional misuse of legal provisions. Investment in cyber labs, training programmes, and victim-sensitive processes is uneven across states.

5.3 Platform cooperation and notice-and-takedown dynamics

Platforms often operate under global policies and face complex incentive structures. The intermediaries' rules push platforms toward quicker removal of flagged content, but inconsistent enforcement, automated moderation errors, and the lack of transparency in platform decisions frustrate victims and may chill legitimate expression.

5.4 Cross-jurisdictional and jurisdictional challenges

Perpetrators may be located in other states or countries, complicating investigation and prosecution. Mutual legal assistance treaties (MLATs), platform data localisation practices, and varying enforcement standards create friction for timely redress.

5.5 Victim support gaps (psychological, legal, technical)

Victims of cyberbullying often need psychological counselling, legal advice, and technical assistance to secure accounts and remove content. Government and non-governmental support systems exist in some regions but are inadequate nationwide.

6. Comparative Perspectives and Models

A review of international approaches reveals several useful practices: clear criminal prohibitions narrowly defined to target serious and repeated harassment; statutory or regulatory duties for platform transparency and appeals; specialist cybercrime courts or divisions; and robust prevention through school curricula and public awareness campaigns. The EU's child-safety-oriented rules and the UK's combination of criminal law with educational measures offer instructive models.

7. Policy and Legal Reform Proposals

This section proposes reforms balanced across constitutional safeguards, victim protection, and practical enforceability.

7.1 Narrowly tailored criminal provisions

Lawmakers should consider crafting narrowly defined offences that criminalise sustained, targeted harassment and threats that cause real-world harm or a significant risk to mental or physical safety. Statutory language should avoid catch-all words like "offensive" and require proof of intent, repetition, or demonstrable harm.

7.2 Specialist cyber units and capacity-building

Expand and professionalise cybercrime units at the state level, invest in digital forensics labs, and build victim-sensitive investigation protocols. Training should include collecting, preserving, and presenting digital evidence, as well as trauma-informed interviewing.

7.3 Safer intermediaries: transparent, accountable notice systems

Intermediaries should be required to publish transparency reports, explain takedown decisions, maintain accessible grievance redressal, and provide expedited channels for content removal involving threats, doxxing, and sexual imagery. Appeal mechanisms should be timely and independently reviewed.

7.4 Victim-centred remedies and civil remedies expansion

Beyond criminal law, strengthen civil remedies: streamlined injunctions for content removal, expedited court processes for urgent takedown requests, and statutory rights to require intermediaries to preserve evidence for a limited period to assist investigations.

7.5 Education, awareness, and school-based prevention

National curricula should incorporate digital citizenship, online consent, and bystander intervention training. Public campaigns and parental resources can reduce incidence and encourage early reporting.

7.6 Data protection and privacy safeguards

Traceability measures and metadata access must be calibrated against privacy rights. Any laws requiring retention or traceability must include strong procedural safeguards, judicial oversight, and limits on scope and retention period.

8. Recommendations (Short, Medium, Long Term)

Short term (0–12 months): - Issue standard operating procedures (SOPs) for police on cyberbullying complaints. - Require platforms to create expedited reporting channels for clear cases of doxxing, threats, and image-based abuse. - Launch targeted training modules for frontline officers and school counsellors.

Medium term (1–3 years): - Enact narrowly tailored amendments or new provisions to criminalise sustained cyber harassment with clear mens rea and actus reus elements. - Establish regional cyber-forensic hubs and victim support centers. - Mandate transparency and audit requirements for large intermediaries.

Long term (3+ years): - Comprehensive review of intermediary liability balancing innovation, speech, and safety. - Embed digital citizenship into national education policy with measurable outcomes. - Create a unified national victim support scheme offering legal, psychological, and technical assistance.

CONCLUSION

Cyberbullying poses multifaceted challenges that intersect law, technology, psychology, and social norms. India's current legal framework offers important tools but also reveals gaps in specificity, enforcement capacity, and victim support. A calibrated approach that combines narrowly tailored laws, stronger enforcement capacity, accountable intermediaries, and prevention through education will be the most effective path forward. Respect for constitutionally protected speech and privacy must remain central to any reform.

REFRENCES

1. Information Technology Act, 2000. Government of India.
2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Ministry of Electronics and Information Technology.
3. Shreya Singhal v. Union of India, Supreme Court of India, Writ Petition (Criminal) No. 167 of 2012 (2015).
4. Indian Penal Code, 1860.
5. Protection of Children from Sexual Offences (POCSO) Act, 2012.
6. National and regional reports on cybercrime, police training initiatives, and NGO resources on online safety.
7. Bansal R. Cyberstalking and online harassment: Legal framework in India. *Indian J Law Technol*. 2020;16(2):45-67.
8. Mehta A. Impact of IT Act amendments on digital abuse cases. *Natl Law Rev*. 2021;14(1):89-112.
9. Sharma D. Legal protection against cyber harassment: A critical analysis. *Int J Cyber Law*. 2019;11(3):55-78.
10. Kohli V. Cybercrime jurisdiction in India: Challenges and solutions. *J Digit Law Ethics*. 2022;18(4):101-29.
11. Roy P. The role of social media in cyberstalking cases: Legal implications. *Indian Law J Technol Soc*. 2021;9(2):77-99.

12. Sinha K. Comparative study of cyber stalking laws in India and the USA. *Harvard Cyber Law J*. 2020;12(1):203-28.
13. Rao M. The evolution of digital abuse laws in India: A decade of change. *Delhi Law Rev*. 2018;20(1):142-63.

About the Authors

Rahul Dev Tyagi is a Research Scholar at Maa Shakumbhari University, Saharanpur, Uttar Pradesh, India. He is involved in academic research, contributing to the advancement of knowledge in his area of study. With a deep commitment to his scholarly work, Rahul aims to explore and expand on critical research topics in his field.

Prof. Dr. Om Dutt is the Head of the Department of Law at D.A.V. P.G. College, Muzaffarnagar, Uttar Pradesh, India. With extensive experience in legal studies, he has played a key role in advancing legal education and research at the institution, fostering academic growth and leadership in the field of law.