CYBERBULLYING AND ONLINE HARASSMENT: LEGAL CHALLENGES AND SOCIAL REALITIES - INDIAN ASPECT

Joe Thomas & A L Krishnapriya, Bharat Matha School of Legal Studies, Choondy Aluva

Introduction

The internet has transformed social life in India. Smartphones, affordable data, and a flourishing social media ecosystem have expanded opportunities for communication, learning, commerce, and civic participation. But alongside these benefits has come a darker reality: cyberbullying, online harassment, doxxing, coordinated trolling, and image-based abuse. These harms affect children and adults, students and professionals, public figures and private citizens. They can cause psychological trauma, reputational damage, financial loss, and, in extreme cases, self-harm. Understanding cyberbullying in India therefore requires a socio-legal lens: one that examines how social factors (culture, family, schools, economic inequalities, and platform design) interact with the legal framework, enforcement capacities, and public policy responses.

This article maps the contours of cyberbullying and online harassment in India. It outlines the forms these harms take, reviews the domestic legal architecture and recent rule-making, examines enforcement and evidentiary challenges, assesses social realities that complicate legal responses, and offers a set of practical recommendations for lawmakers, platforms, schools, and civil society.

1. Defining cyberbullying and online harassment

Cyberbullying refers to intentional and repeated aggressive behavior conducted through digital devices and online platforms with the purpose of harming, humiliating, intimidating, or excluding a person. Online harassment is a broader umbrella that includes bullying but also one-off attacks, doxxing (publishing private information), revenge pornography, coordinated smear campaigns, impersonation, threats, and persistent stalking via messaging platforms or social networks. Both terms capture actions that exploit the affordances of the internet—anonymity, scale, speed, permanence, virality—to magnify harm.

2. Scale and trends in India

Quantifying cyberbullying is difficult because it overlaps with many categories of cybercrime and because many victims do not report incidents. Nevertheless, official crime statistics and international surveys paint a worrying picture: India has seen a steady rise in cybercrimes in recent years, with the

National Crime Records Bureau (NCRB) reporting a significant jump in registered cyber incidents in 2023. The increase is driven largely by fraud and financial exploitation, but categories involving harassment, impersonation, and attempts to cause disrepute are also prominent among recorded offences.

International surveys show that online bullying is widespread among young people; UNICEF's global polls, for example, indicate that roughly one in three young people report being victimized online—an alarming statistic with important implications for India's large youth population.

3. The legal framework in India: statutes and rules

At the center of India's legal response to online harms is the Information Technology Act, 2000 (IT Act), supplemented by provisions in the Indian Penal Code (IPC), the Protection of Children from Sexual Offences Act (POCSO), and procedural laws. Key legal elements include:

• Information Technology Act (2000) and allied rules: The IT Act addresses computer-related offences, authentication, and intermediaries. Several sections of the IT Act criminalize acts such as identity theft, cheating by personation (under sections introduced by amendment), publishing obscene material electronically, and transmission of information that can cause harm. The Central Government has power to frame rules governing intermediaries (platforms), which has led to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021—detailed rules that set due-diligence obligations for intermediaries, grievance redressal requirements, and takedown timelines. (MeitY)

• Indian Penal Code (IPC): Traditional penal provisions apply to many forms of online harassment. For example, offences such as criminal intimidation (Section 503 IPC), defamation (Sections 499–500 IPC), stalking (amendments and reading with other sections), and intentionally causing hurt (Sections 321–324 IPC depending on facts) have been used to prosecute online conduct that would otherwise be considered "offline." Identity theft, cheating, and forgery may also be enforced using IPC provisions in combination with IT Act sections.

• Protection of Children from Sexual Offences Act (POCSO): POCSO addresses sexual exploitation and abuse of minors; image-based sexual abuse, grooming, and online sexual exploitation fall within its ambit when victims are children.

• Case law shaping online speech: A landmark Supreme Court decision—Shreya Singhal v. Union of India (2015)—struck down Section 66A of the IT Act, which had permitted arrests for "offensive" online content and was widely criticized for chilling free speech. The judgement reinforced the importance of safeguarding freedom of expression while permitting reasonable restrictions that are narrowly and clearly defined. The decision remains a critical reference point when balancing speech and protection. (Global Freedom of Expression)

4. How the law addresses cyberbullying: strengths and limits

Strengths:

• Legal coverage across instruments: A combination of IT Act provisions, IPC offences, and special statutes (like POCSO) means that many forms of online harassment can be framed as criminal conduct in India.

• Intermediary rules: The 2021 Intermediary Guidelines require platforms to maintain grievance redressal mechanisms, appoint compliance officers, and follow prescribed takedown timelines—tools that can allow victims to seek rapid content removal without immediately resorting to police complaints. (MeitY)

• Specialized police cells and helplines: Several state police forces have created cybercrime cells and national / state helplines to assist victims, and there has been investment in training and infrastructure to fight cyber-enabled offences.

Limits and gaps:

• Enforcement bottlenecks and capacity constraints: While the legal tools exist, enforcement is uneven—driven by variable resources across police districts, lack of specialized training in digital evidence handling, and inconsistent prosecution outcomes.

• Chilling or insufficiently precise laws (and their past misuse): The striking down of Section 66A illustrated not just a constitutional victory for free speech but also the reality that vaguely worded provisions can be abused to silence dissent or to settle personal scores. Any legislative attempt to tackle cyber harassment must avoid replicating these overbroad formulations.

• Over-reliance on takedowns without remediation: Content removal is important, but takedowns alone do not guarantee accountability for perpetrators, nor do they fully address harms like reputational damage, extortion, or long-term psychological trauma. Victims frequently need legal remedies, mental health support, and mechanisms for evidence preservation.

• Jurisdictional and cross-border challenges: Perpetrators may operate from other states or countries; tracing anonymous accounts and obtaining cross-border cooperation is time-consuming and legally complex.

• Under-reporting: For social and cultural reasons (shame, fear of family repercussions, distrust of police), many victims—especially women and minors—do not report incidents. Under-reporting weakens the ability of statistics and policymakers to accurately assess and respond to the problem.

5. Evidentiary and procedural challenges

Proving online harassment in court often turns on collection, preservation, and authentication of digital evidence. Important hurdles include:

• Ephemeral content and platform policies: Stories, disappearing messages, and ephemeral formats demand immediate action by victims to preserve content. While platforms may retain logs, users often lack the knowledge or capacity to seek or preserve evidence promptly.

• Anonymity and fake profiles: Perpetrators commonly use pseudonymous profiles, multiple accounts, or manipulated images. Tracing an account to a real person may require platform cooperation and, sometimes, telecom or ISP records—processes that involve proper legal channels and can be delayed.

• Chain of custody and admissibility: Digital forensics procedures must be forensic-grade to ensure admissibility. Many police stations lack training in secure evidence collection, which compromises later prosecution.

• Burden of proof and intent: Courts require proof of mens rea or intention in many offences. Proving that a message was sent with the intention to intimidate, humiliate, or harm can be difficult, particularly in borderline cases involving “jokes” or “trolling.”

6. Social realities that complicate legal responses

The effectiveness of legal frameworks depends on social context. Key social realities in India include:

• Stigma and familial pressures: Victims—particularly women and adolescents—often face pressure to avoid public complaints to prevent “dishonor.” This reduces reporting and leads to informal, non-legal remedies that might not stop repeat offenders.

• Digital literacy gaps: While India has hundreds of millions of internet users, digital literacy—understanding privacy settings, reporting tools, and basic security hygiene—varies greatly. Users who are unaware of reporting mechanisms or evidence-preserving steps are more vulnerable.

- School and parental responses: Many schools lack clear anti-bullying policies for online spaces. Parents may be unfamiliar with apps and platforms, limiting their ability to guide or protect children.

- Platform design and attention economy: Social media mechanics (likes, shares, algorithmic amplification) can incentivize sensational or abusive content because it generates engagement. Design choices—such as weak friction in account creation—facilitate mass trolling and harassment.

- Victim-blaming narratives: Public discourse often veers into blaming victims, especially in cases with sexual elements or when the victim is a woman with a public profile. This discourages reporting and re-victimizes those seeking help.

7. Case studies and incident types (illustrative)

- Image-based sexual abuse / "revenge porn": Non-consensual sharing of intimate images is pervasive and causes enduring harm. When victims are minors, POCSO applies; for adults, IPC and IT Act provisions have been invoked. Yet outcomes vary and many victims find takedown and prosecution slow and traumatic.

- Doxxing and outing: Publication of private contact details or family information can trigger threats, extortion, and real-world harm. Tracing the perpetrator often requires cooperation from platforms and telecom providers.

- College/school cyberbullying: Students targeted via group chats or social media can face isolation, depression, and academic decline. Educational institutions sometimes respond with ad hoc measures rather than formal grievance mechanisms.

- Political and gendered trolling: Public figures—especially women in politics or media—face coordinated harassment that blurs political debate with abuse, raising questions about acceptable speech thresholds and platform moderation in a democracy.

8. Platform liability, intermediary duties, and the 2021 rules

The 2021 Intermediary Guidelines were designed to modernize the obligations of platforms operating in India. They require designated intermediaries or large social media services to:

- Appoint grievance redressal officers and publish compliance reports.

- Acknowledge grievances and act on takedown requests within specified timeframes.

- Maintain records and assist law enforcement when legally compelled.

These steps were intended to provide victims with clearer, faster pathways to content removal and redress. However, the rules are not a panacea: compliance quality varies among platforms, and there are continuing debates about the rules' implications for privacy (traceability), freedom of expression, and the technical feasibility of some obligations. (MeitY)

9. Prevention, education, and non-legal remedies

Given the limits of criminal law, prevention and social interventions are critical:

• Digital literacy programs: Teach children, parents, and teachers about privacy settings, secure communication, reporting tools, and evidence preservation. Schools and community centers should integrate age-appropriate modules into curricula.

• School anti-bullying policies: Clear policies that include online behavior, reporting protocols, and restorative approaches can reduce incidents and ensure consistent responses.

• Mental health support: Victims need accessible counseling services; helplines and NGOs can play a bridging role until formal services are available.

• Platform design changes: Social media companies can minimize harm by removing features that enable mass harassment, implementing stronger friction for account creation, enabling more granular blocking and reporting, and investing in moderation teams and AI tools tuned for local languages and contexts.

• Community moderation and bystander intervention: Empowering platform communities to flag abuse and promoting positive norms can reduce the reach of harassing content.

10. Policy recommendations

To better address cyberbullying and online harassment in India, a multi-pronged strategy is necessary:

A. Legal and regulatory reforms

1. Precision over breadth: New legal provisions (or amendments) aimed at online harms should be narrowly drafted to target specific wrongful acts—e.g., non-consensual image distribution, doxxing with malicious intent, persistent cyberstalking—while avoiding vague terms that risk impinging legitimate speech.

2. Faster legally-backed evidence preservation: Introduce streamlined legal mechanisms (court-stamped emergency preservation orders or expeditious judicial oversight) enabling platforms to retain metadata and content temporarily to aid investigations without long delays.

3. Specialist cyber benches or procedures: Encourage special procedures in courts for cyber harassment matters—fast-track adjudication where possible, given the ephemeral nature of online harm and the need for timely remedies.

B. Enforcement and capacity-building

1. Strengthen cyber forensic units across districts, with standardized training in digital evidence handling and chain-of-custody protocols.

2. Institutionalize training for police officers on psychological sensitivity and trauma-informed handling of victims, especially minors and women.

3. Expand public awareness campaigns on reporting avenues (e.g., national helplines), rights, and legal remedies.

C. Platform accountability and design

1. Require transparency reporting by platforms on harassment complaints, takedowns, and outcomes—disaggregated by type of content and region.

2. Promote better safety-by-design practices: friction on account creation, stricter identity verification for high-risk features, improved reporting UI/UX, and quicker human review for urgent harassment cases.

3. Encourage independent audits of platform moderation processes and algorithmic amplification to identify systemic bias or failure modes that enable harassment.

D. Education and social interventions

1. Implement digital citizenship curricula that cover respectful online behavior, consent, bystander intervention, and mental health resources.

2. Support NGOs and school counselors with funding and training to respond to incidents and follow through with restorative justice methods where suitable.

3. Engage parents through community workshops to demystify platforms and teach constructive

supervision without punitive surveillance that erodes trust.

4. Balancing free expression and protection

One of the central tensions in regulating online abuse is balancing free expression rights with the need to protect individuals from harm. India’s constitutional and judicial framework places high value on freedom of speech while allowing reasonable restrictions that are narrowly tailored. The Shreya Singhal decision (2015) remains instructive: laws must be precise, proportionate, and not open to arbitrary application. Policymakers must therefore craft offences and platform obligations that clearly define unlawful conduct while preserving legitimate debate, satire, and dissent. (Global Freedom of Expression)

12. The role of civil society and research

Research into the dynamics of cyberbullying in India—especially with respect to language diversity, rural/urban differences, gendered patterns, and platform-specific behaviors—remains limited. Civil society organizations, academic institutions, and independent researchers should be supported to collect evidence, evaluate interventions, and pilot community-based responses. NGOs also play a vital role in providing immediate support, legal aid, and public interest litigation when systemic failures arise.

13. Practical guidance for victims (a brief primer)

For individuals facing cyberbullying or harassment in India, immediate steps can improve outcomes:

- Preserve evidence: Take screenshots, note timestamps, keep URLs, and collect witness statements where possible.

- Use platform reporting tools: Most major platforms have reporting and blocking features and must respond under the Intermediary Rules.

- File a complaint: If threats, extortion, or sexual exploitation are involved, report to the local police or cybercrime cell. Use national helplines and local NGOs for support.

- Seek interim relief: For image-based abuse, request platform takedowns; consider legal notices or injunctions through a lawyer for faster action in severe cases.

- Access support: Contact counseling services, support groups, and legal aid clinics—psychological recovery is as important as legal redress.

14. Conclusion

Cyberbullying and online harassment are complex problems that straddle law, technology, culture, and human behavior. India's existing laws, the IT Rules, and judicial pronouncements provide a foundation for redress, but practical challenges—enforcement, evidentiary hurdles, social stigma, and platform design—limit their effectiveness. The rapid rise in recorded cyber incidents underscores the urgency of a coordinated response.

A future-ready strategy must combine precise legal reform, stronger enforcement capacity, safety-centred platform design, widespread digital literacy, and accessible support services. Above all, the solution must be holistic: criminal law and takedowns are necessary but not sufficient. Reducing online harm will require changing social norms, creating safer digital spaces by design, and ensuring that victims have timely, trauma-informed access to justice and recovery resources.