

India's Legal Gaps in Tackling Cyberbullying and Online Abuse

May 18, 2025 • vajiramandravi.com

Cyberbullying Laws in India Latest News

- In the wake of the Pahalgam terror attack, Himanshi Narwal, widow of Navy Lieutenant Vinay Narwal, faced severe online abuse after appealing for peace and rejecting anti-Muslim sentiment.
- Similarly, Foreign Secretary Vikram Misri was trolled for announcing a ceasefire understanding with Pakistan, leading him to lock his X (formerly Twitter) account.
- These incidents highlight how anonymous online trolls often target individuals who challenge dominant narratives.
- To address this growing menace, regulatory reforms are needed to ensure accountability and curb impunity in digital spaces.

Rise of New-Age Cybercrimes

- Modern cybercrimes such as cyberbullying, stalking, hate speech, and doxxing have become rampant.
- **Doxxing**—publicly revealing private information like addresses or phone numbers—often leads to real-world harassment and threats.

Disproportionate Impact on Women and Minorities

- Research indicates that online abuse frequently targets women and minorities, often driven by coordinated political motives.
- The abuse can escalate to rape and death threats, highlighting the gravity of the issue.

Gaps in India's Legal Framework

- India lacks a specific law to address online hate speech and trolling.
- Instead, it relies on general provisions under the **Bharatiya Nyaya Sanhita (BNS), 2003**, and the **Information Technology (IT) Act, 2000**.
- Key relevant sections include:
 - **BNS**: Section 74 (outraging modesty), 75 (sexual harassment), 351 (criminal intimidation), 356 (defamation), and 196 (promoting enmity).
 - **IT Act**: Section 66C (identity theft), 66D (impersonation), and 67 (obscene content).

Structural Limitations and Need for Reform

- Legal experts argue that while the framework is partially functional, it fails to address collective online harassment or sustained abuse that isn't clearly obscene or threatening.
- Laws like stalking under BNS are gender-specific and don't account for mob-led digital abuse.
- Provisions like defamation or intimidation require proof of threat or reputational damage, which are often inadequate in the fast-paced, anonymous world of online trolling.

India's Legal Tools

- In India, **Section 69A of the IT Act** allows the government to block online content in the interest of public order, national security, or foreign relations.
- Non-compliant platforms risk losing **safe harbour protection under Section 79**, which otherwise shields them from liability for user content.

Concerns Over Online Censorship

- Experts caution that these provisions, especially Section 69A, are being misused for censorship.
- The Supreme Court's 2015 Shreya Singhal judgment upheld Section 69A but required transparent procedures and reasons for takedowns — a principle often violated, as seen after the Pahalgam attack, when over 8,000 accounts were blocked without proper explanation.

Legal Pushback and Lack of Clarity

- X has legally challenged the government's use of Section 79(3)(b), which lacks a clear definition of "unlawful acts" and has no review mechanism, unlike Section 69A.
- The lawsuit argues that procedural safeguards are being bypassed.

Reconsideration of Safe Harbour

- India's Ministry of Information and Broadcasting is now reconsidering the continuation of safe harbour protections for platforms, citing the growing challenge of combating fake news and disinformation.

Doxxing and Associated Challenges

- In February 2023, the Delhi High Court ordered X (formerly Twitter) to remove tweets that exposed the personal and professional information of a woman who had criticized Uttar Pradesh CM.
- Despite acknowledging privacy violations, the court ruled that the act did not amount to doxxing, as the information was already publicly available.

Doxxing Not a Statutory Offence—Yet a Privacy Threat

- Experts highlight that doxxing poses a serious threat and violates the right to privacy.
- Although it is not a statutory crime in India, civil remedies under tort law may still be pursued.

Legal Ambiguity Over 'Publicly Available' Data

- The Digital Personal Data Protection (DPDP) Act, 2023 excludes personal data from its protection if the data is “publicly available.”
- However, this term remains undefined, leaving room for misinterpretation and potential misuse.

Risk of Cybercrimes Due to Legal Loopholes

- The vague definition of “publicly available data” in the DPDP Act can enable cybercrimes like doxxing.
- In the digital age, even fragmented pieces of data across platforms can be easily aggregated to target individuals, raising serious privacy and safety concerns.

Other Challenges

- **Enforcement Remains the Weakest Link**
 - Experts agree that poor enforcement, not the absence of laws, often prevents victims from receiving justice.
 - Government directives are swiftly implemented, but ordinary users reporting harassment rarely receive timely redress.
- **Gendered Abuse and Institutional Apathy**
 - According to experts, victims of gender-based online abuse face disbelief and victim-blaming.
 - With minimal institutional support and public awareness, legal options become a last resort, leading to psychological and legal trauma.
- **Legal and Structural Barriers to Justice**
 - Analysts highlighted critical challenges like anonymity of offenders, jurisdictional complexity, and inadequate cybercrime training.

Cyberbullying Laws in India FAQs

Q1. Why is cyberbullying rising despite existing laws?

Ans. Current laws are outdated, vague, and poorly enforced, allowing online abuse to persist unchecked.

Q2. What legal provisions currently address online abuse in India?

Ans. Sections from BNS and IT Act cover defamation, intimidation, obscene content, and identity theft, but remain insufficient.

Q3. What is doxxing, and is it illegal in India?

Ans. Doxxing involves disclosing private data online; it’s not yet a statutory crime but violates privacy rights.

Q4. What challenges hinder enforcement of cyber laws?

Ans. Lack of training, jurisdictional issues, anonymity, and institutional apathy make justice difficult for cyber abuse victims.

Q5. Are social media platforms held accountable for content?

Ans. Under Section 69A and 79 of the IT Act, platforms can lose protection if they ignore takedown directives.

Source: TH

Source: <https://vajiramandravi.com/current-affairs/indias-legal-gaps-in-tackling-cyberbullying-and-online-abuse/>

© Vajiram & Ravi. For personal use only.