Cyberbullying Laws in India

Posted at: 19/05/2025

Cyberbullying Laws in India: Rising Threats, Legal Loopholes, and the Urgent Need for Reform

Introduction

Recent incidents involving online harassment of public figures like **Himanshi Narwal**, widow of Navy Lieutenant Vinay Narwal, and **Foreign Secretary Vikram Misri**, have brought renewed attention to the growing problem of **cyberbullying and online abuse in India**. Both individuals were targeted for expressing views that challenged dominant political narratives. These cases highlight a troubling trend—**anonymous online trolls targeting individuals with hate, abuse, and threats**, especially on sensitive issues.

As online platforms become central to public discourse, **cybercrimes like trolling, doxxing, cyberstalking, and online threats** have become widespread. Legal experts, civil society, and victims are calling for urgent **regulatory reforms** to ensure greater accountability and user protection in digital spaces.

Emergence of New-Age Cybercrimes

Modern digital crimes have evolved far beyond traditional hacking or fraud. They now include:

- **Cyberbullying and Trolling:** Repeated, targeted online abuse meant to intimidate or shame individuals.
- **Cyberstalking:** Persistent digital surveillance and harassment, especially of women.
- **Hate Speech:** Online content meant to incite hatred based on religion, caste, gender, or political belief.
- **Doxxing:** Public release of someone's personal information (like address, phone number, or workplace) without consent, often leading to **real-world threats and harassment**.

Disproportionate Impact on Women and Minorities

Multiple studies and reports confirm that **women, minorities, and dissenting voices** are the most frequent targets of cyber abuse.

- Online abuse often escalates to **rape threats, death threats, and character assassination**.
- In many cases, such abuse is **coordinated and politically motivated**, and is amplified by anonymous accounts or bot networks.
- Victims face **psychological trauma** and **reputational damage**, often without meaningful recourse.

India's Legal Framework: Current Status

India does **not yet have a specific law** that directly addresses cyberbullying or online hate speech. Instead, it relies on **general provisions** under:

1. Bharatiya Nyaya Sanhita (BNS), 2023

- **Section 74:** Outraging the modesty of a woman
- **Section 75:** Sexual harassment
- **Section 351:** Criminal intimidation
- **Section 356:** Defamation
- **Section 196:** Promoting enmity between groups

2. Information Technology (IT) Act, 2000

- **Section 66C:** Identity theft
- **Section 66D:** Impersonation using computer resources

AKKA IAS ACADEMY www.akkaias.com Dr. Shivakumar's

- **Section 67:** Publishing obscene content online

3. **Section 69A of the IT Act**

- Allows the government to **block online content** in the interest of **national security, public order, or foreign relations**.

4. **Section 79 of the IT Act**

- Provides **"safe harbour" protection** to social media platforms from liability for user-generated content, unless they fail to act on unlawful content once informed.

Structural and Legal Limitations

While these laws offer some level of protection, they fall short in many key areas:

- There is **no provision** to address **mob-led digital harassment** or **coordinated abuse** from multiple anonymous users.
- Laws like **stalking** are **gender-specific**, excluding male or non-binary victims.
- **Defamation and intimidation laws** require proof of damage or credible threat, which is often difficult to establish online.
- The law lacks clarity on **"publicly available" data**, making enforcement against **doxxing** difficult.

Government Regulation vs. Online Freedom

Following the **Pahalgam terror attack**, the government reportedly blocked over **8,000 accounts** under **Section 69A**, raising questions about transparency. While the **Supreme Court's 2015 Shreya Singhal judgment** upheld Section 69A, it mandated that any content takedown must follow due process and provide reasons.

Despite this, there have been cases where content was taken down or accounts were blocked without sufficient explanation. Critics argue that **content moderation often lacks transparency**, and is sometimes used to silence dissent rather than protect users.

AKKA IAS ACADEMY www.akkaias.com Dr Shivakumar

Legal Pushback by Platforms

Social media platform **X (formerly Twitter)** has legally challenged the government's overuse of **Section 79(3)(b)**, which requires platforms to remove content related to "unlawful acts." The platform argued that the term is **vague and undefined**, and that there is **no formal review mechanism** unlike with Section 69A.

Doxxing: A Growing Concern with No Clear Law

Doxxing, or the public disclosure of personal data without consent, is becoming increasingly common, especially against critics and whistleblowers.

- In a notable 2023 case, the **Delhi High Court** ordered the removal of tweets that revealed personal data of a woman who had criticised a Chief Minister.
- The court, however, ruled that since the information was already **"publicly available"**, it did not qualify as illegal doxxing.

This reflects a major **legal gap**, as **India does not consider doxxing a statutory offence**, despite it being a serious violation of privacy and personal safety.

The Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act was meant to secure user privacy, but it **excludes from protection any personal data that is "publicly available."** Since this term remains **undefined**, it creates a loophole. Even fragmented personal details available online can be aggregated and misused for targeted harassment, yet **the law does not consider this a crime**.

Challenges in Enforcement

- **Weak Police Response:** Victims often face **slow or no response** when reporting cyber abuse.
- **Lack of Training:** Many law enforcement officials are not adequately trained in dealing with cybercrime.
- **Jurisdictional Issues:** Online crimes cross state and even national boundaries, making enforcement complicated.
- **Gender Bias:** Women who report cyber abuse are often not taken seriously, facing **victim-**

blaming and institutional apathy.

Conclusion and the Way Forward

The rise of **cyberbullying, trolling, hate speech, and doxxing** represents one of the most pressing challenges of the digital age in India. Despite having some legal provisions in place, **India lacks a dedicated, comprehensive law** to address the unique nature and scale of **online harassment**.

To effectively counter this threat, the following steps are urgently needed:

- Enact a **dedicated cyberbullying and digital harassment law**, covering gender-neutral and mob-led abuse.
- Define **doxxing as a punishable offence**, regardless of whether data was previously available online.
- Establish **clear, transparent protocols** for content removal under Section 69A.
- Improve **training of police and judicial officers** to handle digital crimes effectively.
- Ensure **support systems for victims**, especially women and marginalised groups, including legal aid, counselling, and safe reporting channels.

As digital spaces continue to shape public discourse and personal identity, **strengthening laws, accountability, and enforcement** is vital to protect individual rights and uphold the democratic values of free speech and dignity.

AKKA IAS ACADEMY
www.akkaias.com
Dr. Shivakumar