The Hindu 18.05.2025

How is cyberbullying tackled under the law?

In the absence of a dedicated law to take on cyber crimes, what are the provisions under the Bharatiya Nyaya Sanhita, 2023, and the Information Technology Act, 2000? Where is the existing regulatory framework lacking? Where do the courts stand?

Aaratrika Bhaumik

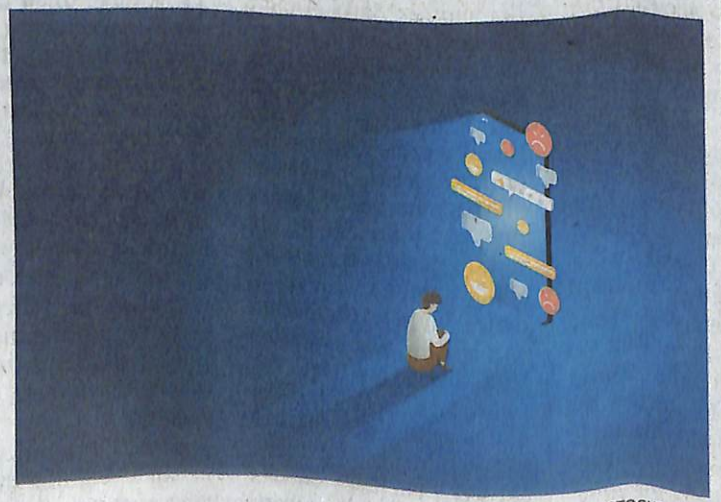
The story so far:

In the wake of the Pahalgam terror attack, Himanshi Narwal, the wife of slain Navy Lt. Vinay Narwal, issued an appeal for peace, rejecting the vilification of Muslims and Kashmiris. However, her message triggered a wave of vicious trolling on X. Similarly, after Foreign Secretary Vikram Misri announced on May 10 that India and Pakistan had reached an understanding to halt military hostilities, his account was flooded with abusive messages, with many targeting even his daughter.

What are the limitations of the existing laws?

A range of terms have emerged to describe forms of cybercrime, including cyberbullying, stalking, and doxxing. Doxxing, short for "dropping dox" (documents), involves the unauthorised release of private information, exposing victims to harassment and real-world threats. Studies show such abuse disproportionately affects women and minorities. India lacks a dedicated law to address online hate speech and trolling. Instead, a few provisions under the Bharatiya Nyaya Sanhita (BNS), 2023, and the Information Technology (IT) Act, 2000, cover certain aspects of cyberbullying. The BNS includes provisions such as Section 74 (assault or criminal force against a woman with intent to outrage her modesty), Section 75 (sexual harassment), Section 351 (criminal intimidation), Section 356 (defamation), and Section 196 (promoting enmity between groups). The IT Act supplements these offences with provisions like Section 66C (identity theft), Section 66D (impersonation fraud), and Section 67 (publishing or transmitting obscene material electronically). "The existing regulatory framework is functional but far from complete. No provision squarely criminalises sustained online abuse that does not qualify as 'obscene,' 'threatening,' or 'fraudulent.' While cyberbullying may sometimes be shoehorned into offences like criminal intimidation or defamation, these require proof of threat or reputational harm and are ill-suited to counter the rapid, anonymous abuse unleashed by online mobs," Apar Gupta, advocate and founder-director of the Internet Freedom Foundation, told *The Hindu*.

'No provision squarely criminalises sustained online abuse that does not qualify as obscene, threatening, or fraudulent'



ISTOCKPHOTO

What are the concerns over censorship?

In India, Section 69A of the IT Act empowers the government to issue blocking orders on grounds aligned with constitutionally permissible speech restrictions, such as sovereignty, friendly relations with foreign States, and public order. Platforms that fail to comply risk losing safe harbour protection under Section 79, which ordinarily shields intermediaries from liability for user-generated content. However, experts have warned that these provisions are increasingly being used for censorship. The government has often removed content without notifying affected users, violating the Supreme Court's 2015 ruling in *Shreya Singhal versus Union of India*. While the court upheld the constitutionality of Section 69A, it underscored that blocking orders must be accompanied by cogent reasons to enable judicial scrutiny. After the Pahalgam attack, X disclosed that it had been directed to block 8,000 accounts in India but said that the government had not specified which posts violated the law in most cases.

In March, X filed a lawsuit in the Karnataka High Court against the Centre's use of Section 79(3)(b) of the IT Act for takedown orders, arguing it circumvents safeguards under Section 69A. Unlike Section 69A, Section 79(3)(b) lacks clear definitions of "unlawful acts" and any review mechanism. Meanwhile, the Ministry of Information and Broadcasting has recently informed a parliamentary committee that it is reviewing safe harbour protections to better tackle "fake news."

What about judicial interventions?

In February last year, the Delhi High Court ordered X to remove tweets revealing the personal and professional details of a woman who reportedly posted a critical comment about Uttar Pradesh Chief Minister Yogi Adityanath. The post triggered a wave of online harassment, with details of her workplace, residence, and photographs being widely circulated. Although these disclosures raised privacy concerns, Justice Prathiba Singh ruled that the incident did not constitute doxxing, as the information was already publicly available. However, the judge acknowledged that doxxing, though not yet a statutory offence in India, poses a serious threat. Accordingly, X was directed to disclose subscriber information associated with the offending posts. This case highlights the contested nature of what qualifies as public information. The Digital Personal Data Protection Act, 2023, exempts from regulation personal data that is made "publicly available", either by the individual concerned or by an entity under a legal obligation. However, it does not define what qualifies as "publicly available data." This lack of clarity may inadvertently enable cybercrimes such as doxxing, given the ease with which fragmented data from multiple platforms can be easily aggregated and used for harassment or intimidation.

What are the challenges ahead?

Experts underscored that enforcement, or rather the lack of it, often determines whether victims can access remedies. "All laws are only as effective as their enforcement. While posts and accounts are promptly removed when government directives are issued, the same urgency is rarely extended to ordinary users reporting harassment or abusive content", Mishi Choudhary, technology lawyer and digital rights advocate, told *The Hindu*. Mr. Gupta agreed, highlighting challenges such as perpetrator anonymity, cross-jurisdictional hurdles, and limited cybercrime training.