INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 13 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 13 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-13-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ONLINE HARRASMENT AND LEGAL GAPS IN DIGITAL PROTECTION

AUTHOR - SHAIK KHAJA GHAREEBAN NAWAZ S, LLM[CRIMINAL LAW] STUDENT AT CRESCENT SCHOOL OF LAW, B.S.ABDUR RAHMAN CRESCENT INSTITUTE OF SCIENCE AND TECHNOLOGY, VANDALUR ,CHENNAI.

BEST CITATION - SHAIK KHAJA GHAREEBAN NAWAZ S, ONLINE HARRASMENT AND LEGAL GAPS IN DIGITAL PROTECTION, THE UNITED KINGDOM, AND THE UNITED STATES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (13) OF 2025, PG. 268-273, APIS – 3920 – 0001 & ISSN - 2583-2344.

INTRODUCTION

In the digital age, social media, online forums, and instant messaging platforms have revolutionized communication, offering unprecedented opportunities for connection and expression. However, this same digital landscape has also become a breeding ground for online harassment—ranging from cyberbullying and stalking to doxxing and hate speech. Victims often face emotional distress, reputational harm, and even physical threats as harassment transcends the boundaries of the virtual world.

Despite the growing prevalence of these abuses, many legal systems struggle to keep pace with technological change. Existing laws often lack the clarity or scope to address digital misconduct effectively, leaving victims without adequate protection or recourse. Gaps in jurisdiction, enforcement challenges, and the anonymity afforded by the internet further complicate accountability. As a result, there is a pressing need to reassess and strengthen legal frameworks to ensure that digital spaces are as safe and just as their physical counterparts.

The rise of digital communication has brought people closer together but has also created new forms of abuse, including online harassment, cyberbullying, and stalking. Victims often face serious emotional and social harm, yet many legal systems remain ill-equipped to address these issues. Gaps in digital protection laws and enforcement leave individuals vulnerable, highlighting the urgent need for stronger and clearer legal responses to online harassment.

The digital age has transformed communication, enabling instant connectivity and the widespread sharing of information. However, this evolution has also amplified malicious online behaviours, particularly digital defamation and cyber harassment. These phenomena pose significant legal and social challenges, often leaving victims struggling for redress in a rapidly evolving digital landscape.

For instance, the cyberbullying of actress Rhea Chakraborty, following the death of Sushant Singh Rajput, highlighted how online platforms can turn into breeding grounds for defamatory and harassing behaviour. Social media trials and baseless accusations against her exemplified how unchecked digital abuse can devastate reputations and mental health, sparking debates about stricter cyberbullying laws.

Similarly, the recent incidents such as targeted trolling of journalist Rana Ayyub for her opinions, a 16-year-old queer makeup artist facing severe homophobic bullying on Instagram after a viral post, and rising misuse of AI tools for harassment, emphasize the need for robust protections to ensure dignity and safety in the digital space.

With the recent overhaul of India's criminal laws under the Bharatiya Nyaya Sanhita, 2023 (BNS), there is a need to explore how the legal

framework addresses these challenges and how it can be further strengthened to ensure accountability in cyberspace.

What Constitutes Digital Defamation and Cyber Harassment?

Digital defamation refers to the act of publishing false and damaging statements about an individual or entity online. While defamation in its traditional sense is well-defined under Indian law, its digital counterpart takes unique forms, such as defamatory posts on social media, blogs, or emails. Under the Bharatiya Nyaya Sanhita, 2023, such offences are codified under Section 354, replacing the earlier Section 499 of the Indian Penal Code. The instantaneous and farreaching impact of digital defamation makes it a potent tool for reputational harm.

Cyber harassment encompasses a spectrum of online behaviours designed to intimidate, humiliate, or harm individuals. These include cyberstalking, trolling, doxxing (publishing private information without consent), and the sharing of morphed or non-consensual images. Provisions under the BNS, such as Section 354F (cyberstalking) and Section 354H (insult to modesty), alongside sections of the Information Technology Act, 2000, provide legal recourse for victims of such harassment.

The Legal Framework

India has established a robust legal framework to address cybercrimes, primarily through the Information Technology Act, 2000 (IT Act) and subsequent amendments.

Under the IT Act, provisions such as Section 66C deals with identity theft which directly address specific online offenses and Section 66E criminalizes the publication of private images without consent, while Section 67 and 67A penalize the transmission of obscene or sexually explicit material. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate social media platforms to establish grievance redress mechanisms, ensuring swift action against harmful content.

Complementing these are legal provisions from the Bharatiya Nyaya Sanhita, 2023 (BNS). Importantly, cybercrimes have now been classified as an "organized crime" under Section 111 of the BNS. Additionally, Section 77, 78 and 79 of the BNS deals with cases assault against women i.e., voyeurism, stalking, and any word, gesture or act intended to insult modesty of a woman respectively.

Furthermore, Section 351 deals with criminal intimidation, Section 352 pertains to intentional insult with intent to provoke breach of peace and Section 356 has expanded the scope of defamation to counteract emerging challenges. Moreover, the Protection of Children from Sexual Offenses Act, 2012 (POCSO) extends safeguards to minors against sexual abuse and exploitation online. Collectively, these laws aim to balance the right to free speech with the need for accountability and protection in the digital domain.

Interestingly, the Supreme Court through its landmark judgment Shreya Singhal v. Union of India (2015) 5 SCC 1, struck down Section 66A of the IT Act which was deemed unconstitutional for curbing free speech. Yet, this judgment inadvertently created a vacuum in addressing online abuse, as Section 66A had provisions to tackle offensive or menacing messages online. This gap has left victims of cyber harassment, especially those targeted by coordinated online campaigns, with limited legal recourse.

Key Challenges in Addressing Digital Defamation and Cyber Harassment

One of the primary challenges in addressing digital offenses is jurisdictional ambiguity. The internet transcends geographical boundaries, and cases often involve perpetrators or servers located outside India. Determining the jurisdiction for legal proceedings and enforcing remedies in such scenarios can be complex and time-consuming.

Another significant hurdle is the anonymity of offenders. Cybercriminals often exploit tools and techniques to mask their identities, making

it difficult for law enforcement to trace them. Although investigative agencies possess advanced technologies to identify offenders, delays in cooperation from social media platforms and intermediaries often impede swift resolution.

The challenge of balancing free speech with accountability also persists. India's constitutional right to free speech under Article 19(1)(a) must be weighed against the need to protect individuals from defamation and harassment. Overregulation risks stifling legitimate expression, while under regulation may fail to safeguard victims.

Additionally, India's overburdened judiciary struggles to handle the increasing volume of cybercrime cases. Limited infrastructure and technical expertise within the judiciary lead to delayed adjudication, leaving victims vulnerable and offenders unpunished. Compounding these issues is the lack of public awareness, as many victims remain unaware of their legal rights or hesitate to report incidents due to stigma or fear of reprisal.

Thus, the global and evolving nature of cybercrimes complicates prosecution and the victims often encounter frustration due to these impediments.

Strengthening the Response to Digital Defamation and Cyber Harassment

To combat digital defamation and cyber harassment effectively, there is a pressing need to enhance legislative provisions. The IT Act should be updated to explicitly address emerging forms of cyber harassment, such as doxxing and deepfake technologies. Additionally, a dedicated statute for digital defamation can provide a unified framework for addressing these issues, incorporating both civil and criminal remedies for victims.

The social media platforms and online intermediaries must be held accountable and they should mandatorily deploy advanced AI tools to monitor harmful content which is circulated online. A robust mechanism for swift removal of defamatory or harassing material upon being reported, along with stringent penalties for non-compliance, can ensure that platforms act responsibly. Collaborative efforts between regulators and intermediaries can further enhance transparency and efficiency.

Specialized cybercrime units are critical for tackling the anonymity of offenders. Establishing such units at the state and district levels, equipped with cuttingedge forensic tools, can expedite the tracing of offenders. National helplines and support networks can also empower victims to report offenses and seek assistance without fear or hesitation.

Judicial reforms are equally essential such as, training judicial officers on the nuances of digital evidence and emerging cyber laws can enhance their ability to adjudicate cases effectively. Setting up fast-track courts for cybercrime cases can further ensure timely justice and act as a deterrent for offenders.

Public awareness campaigns and large-scale digital literacy initiatives can educate citizens about safe online practices and available legal remedies. Collaborating with social media platforms and educational institutions to promote ethical digital behaviour can foster a culture of responsibility and respect in cyberspace.

India's Legal Gaps in Tackling Cyberbullying and Online Abuse

Cyberbullying Laws in India

In the wake of the Pahalgam terror attack, HimanshiNarwal, widow of Navy Lieutenant Vinay Narwal, faced severe online abuse after appealing for peace and rejecting anti-Muslim sentiment.

Similarly, Foreign Secretary VikramMisri 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.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

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.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

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.

Findings

1. **Limited awareness of digital protection laws**
   Many law students and advocates noted that both victims and even some legal professionals have limited understanding of existing cybercrime provisions. This lack of awareness leads to underutilization of legal remedies available for online harassment.
2. **Perception of outdated legislation**
   Respondents emphasized that current cyber laws do not adequately address newer forms of online abuse—such as identity theft through AI tools, deepfake pornography, and non-consensual sharing of private content. They felt that existing provisions under general penal codes are insufficient for digital contexts.
3. **Weak enforcement mechanisms**
   Law students and advocates agreed that enforcement remains a major barrier. Even when laws exist, delays in cybercrime investigations, lack of technical expertise, and poor coordination between law enforcement and digital platforms hinder justice.
4. **Inconsistent platform accountability**
   Many participants highlighted that online platforms (social media sites and messaging apps) often fail to act swiftly on harassment complaints. The absence of clear legal obligations for these intermediaries creates a loophole that allows offenders to continue abusive behavior online.
5. **Victim reluctance and stigma**
   Advocates observed that victims—especially women and youth—often choose not to report online harassment due to fear of social backlash, lengthy procedures, or the belief that authorities will not act effectively.
6. **Need for specialized legal and technical training**
   Both groups pointed out the gap in professional preparation, emphasizing that law schools and bar associations rarely provide specialized education in cyber law or digital evidence handling.

7. **Call for victim-centered legal reform**
Respondents commonly suggested that current laws focus more on punishment than protection, and there should be mechanisms for immediate relief—like faster takedowns and restraining orders.

Recommendations

1. **Draft a comprehensive Digital Harassment Act**
Establish a dedicated law defining various online harassment offenses and prescribing both preventive and punitive measures, with clear jurisdictional and evidentiary guidelines.
2. **Integrate cyber law education in legal curricula**
Encourage law schools to include mandatory courses on digital law, online harassment, and cyber forensics to better prepare future legal professionals.
3. **Strengthen institutional enforcement**
Create specialized cyber investigation units equipped with digital forensic experts and ensure coordination with prosecutors trained in online harassment cases.
4. **Mandate accountability for online platforms**
Require social media and tech companies to adopt transparent complaint-handling mechanisms, immediate content removal procedures, and cooperation with legal authorities.
5. **Develop accessible reporting and support systems**
Launch centralized reporting portals and victim support centers offering legal assistance, counseling, and protection for high-risk individuals.
6. **Promote digital literacy and awareness campaigns**
Implement national campaigns targeting schools, universities, and workplaces to inform users about their rights and legal options against online abuse.
7. **Enhance legal aid and victim protection measures**
Provide free legal assistance, faster injunctions, and emergency restraining orders for victims facing ongoing digital threats.
8. **Encourage ongoing legislative review**
Establish a policy mechanism to periodically update digital protection laws in response to emerging technologies and evolving online threats.

Conclusion: Towards a Safer Digital Landscape

Digital defamation and cyber harassment represent significant threats to personal dignity, reputation, and privacy in an increasingly online world. While India's legal framework provides a foundation to address these challenges, continuous evolution is necessary to keep pace with technological advancements and emerging threats.

As professionals, businesses, and individuals, we must remain vigilant about our digital presence, leveraging the legal protections available to ensure our safety and reputation. Policymakers and law enforcement agencies must adopt a multi-stakeholder approach to strengthen laws, expedite enforcement, and build public awareness.

By fostering accountability, enhancing victim-centric remedies, and promoting ethical digital behaviour, India can create a secure and empowering digital environment for all. The digital age holds immense potential, and it is through collective effort that we can ensure this potential is realized responsibly.