Gaps in Legislation Addressing Online Abuse & Harassment in India

N. Amuthalakshmi, Assistant Professor, School of Law, VISTAS.

amuthalakshmi.law@vistas.ac.in

INTRODUCTION

Gaps in Legislation Addressing Online Abuse and Harassment in India

With the advent of the digital age, India has seen a rapid expansion of online platforms, making it easier for people to connect, share information, and express themselves. However, alongside the growth of these digital spaces, there has been a parallel rise in online abuse and harassment, particularly against women, minorities, and vulnerable groups. While the Indian government has made some efforts to address online harassment, gaps in the existing legislation still leave many victims without adequate protection. In this article, we explore these gaps and their implications for those experiencing online abuse.

1. Inadequate Legal Framework for Online Abuse

One of the biggest gaps in India's response to online abuse is the lack of a comprehensive legal framework that specifically addresses the nuances of cyber harassment. Existing laws related to online abuse, such as Section 66A of the Information Technology Act (which criminalized offensive messages), have either been struck down by the Supreme Court or are insufficient in their coverage. While provisions under the Indian Penal Code (IPC) and the Information Technology Act do touch on certain aspects of cybercrimes (such as cyberbullying, defamation, and stalking), they do not fully capture the range of behaviors associated with online harassment.

For example, laws around defamation or obscenity often fail to recognize the emotionally damaging effects of online abuse that are not always linked to tangible harm (e.g., loss of reputation or physical threats). These gaps leave many cases of harassment unaddressed and often fail to take into account the more complex dynamics of online harm, such as doxxing, trolling, and digital misogyny.

2. Slow and Inadequate Enforcement

Even when laws exist, enforcement remains a significant challenge. The process for victims to file complaints and report cybercrimes is cumbersome and often requires technical expertise that many victims may not have. Additionally, many law enforcement officers are not sufficiently trained to deal with the complexities of cybercrimes, resulting in poor investigation and delayed responses. In some cases, victims face indifference or even victim-blaming from police personnel when they attempt to report online harassment.

Moreover, while social media platforms are frequently the source of online abuse, they are not always held accountable for the content shared by users. Although there have been attempts to regulate these platforms (such as the 2021 IT Rules), the implementation of these regulations has been patchy, and the platforms themselves often do not prioritize the swift removal of harmful content or the protection of victims. This delay in action can exacerbate the emotional and psychological toll on victims of online harassment.

3. Gender-Specific Violence and Digital Misogyny

A particularly disturbing trend in online abuse is the gendered nature of harassment, with women, in particular, facing a disproportionate amount of abuse. This includes everything from unsolicited sexual content and revenge porn to threats of violence and rape. The existing laws in India do not adequately address the specific ways in which women are targeted online. While there are provisions for sexual harassment under the IPC, these laws often fail to recognize the unique nature of online abuse, where perpetrators can harass victims anonymously, making it harder for law enforcement to track and prosecute them.

The absence of gender-sensitive guidelines for dealing with online abuse exacerbates the problem. For example, while the government has taken steps to regulate online platforms, such as the requirement for social media companies to remove content within a specified timeframe, there is little focus on how to protect women from online harassment. This is evident in the widespread nature of "slut-shaming" and "revenge porn," which remain rampant despite legal frameworks in place to prevent them.

4. Lack of Clear Guidelines for Social Media Platforms

While the Indian government has introduced several regulations aimed at improving accountability for digital platforms (e.g., the 2021 IT Rules), there is still no clear, consistent approach to ensuring that these platforms are actively working to combat online harassment. The rules mandate the appointment of grievance officers and require social media companies to comply with takedown requests. However, the enforcement of these regulations remains weak, and there is little oversight to ensure that platforms are adequately addressing the needs of harassment victims.

Moreover, many of the complaints related to online abuse fall under grey areas, where the legal definitions are unclear, and social media platforms are left to interpret the rules at their discretion. Without clear-cut rules or strong penalties for non-compliance, platforms may continue to neglect their duty to protect users from harm, leaving victims vulnerable.

5. Challenges in Cyber security and Data Protection

India’s cyber security infrastructure is still developing, and the protection of user data is not as robust as it should be. Cyber harassment often involves the misuse of personal information, and the lack of adequate data protection laws allows perpetrators to exploit this vulnerability. While the Personal Data Protection Bill has been proposed, it is still not law, leaving individuals exposed to potential abuse. Cybercrimes related to identity theft, cyber stalking, and extortion thrive in this environment, as there are limited mechanisms to prevent or deter the abuse of personal data online.

Additionally, the rise of AI and deep fake technology presents new challenges in ensuring the security of personal data and preventing its misuse. Legislation in India is yet to catch up with the pace at which technology is evolving, further exacerbating the vulnerability of individuals to cybercrimes.

6. Lack of Public Awareness and Digital Literacy A significant issue contributing to online abuse in India is the low level of digital literacy. Many people, particularly in rural areas, are not equipped with the knowledge to understand the

dangers of online platforms or to protect themselves from potential harm. This lack of awareness makes them easy targets for online predators and abusers.

Government initiatives aimed at increasing digital literacy and awareness about cybercrimes are still in their infancy, and while there are some educational campaigns, they are not widespread enough to reach the vast majority of internet users. Without proper education, individuals remain unaware of their rights or how to seek help when they are subjected to online harassment.

Under Indian law, online abuse and harassment are generally addressed through a combination of provisions under the Indian Penal Code (IPC), the Information Technology Act, 2000, and other relevant statutes. Here are key definitions and sections related to online abuse and harassment:

1. Indian Penal Code (IPC)

Section 354A: This section deals with sexual harassment and includes unwelcome physical contact, demand or request for sexual favors, and sexual remarks made online or through other means.

Section 503: This section defines criminal intimidation, which can be used if someone is harassed or threatened online with the intent to cause fear or harm.

Section 499-500: These sections relate to defamation, which includes the act of posting false, derogatory, or defamatory content online.

Section 509: This covers word, gesture, or act intended to insult the modesty of a woman, including online forms of abuse.

Bharatiya Nyaya Sanhita (BNS) 2023

Replacing the IPC, the BNS 2023 introduces updated provisions under the **Section 74** has addresses the sexual harassment, including online harassment such as sending obscene messages or making sexually explicit advances. **Section 75**: punishes following crimes such as cyber stalking, including persistent online contact or monitoring of a woman's digital communications. **Image-Based Sexual Abuse s**pecifically targets the non-consensual sharing of intimate images, commonly known as "revenge porn against innocent women on cyberspace.

2. Information Technology Act, 2000 (IT Act)

Section 66A (Note: This was struck down by the Supreme Court in 2015 for being unconstitutional, as it was deemed overly vague and a threat to freedom of speech).

Section 66C: This deals with identity theft, such as when someone uses another person’s information or impersonates them online without consent.

Section 66E: Involves the violation of privacy, including the sharing of private pictures or videos without consent.

Section 67: Criminalizes the publishing or transmitting obscene material in electronic form, including online harassment related to explicit content.

3. The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013

This Act, though primarily focused on the workplace, applies in cases where the online harassment occurs in a professional context, particularly when the harassment involves sexual advances, offensive comments, or digital threats.

Online Harassment and Abuse in General

Online abuse or harassment can include cyberbullying, trolling, impersonation, threats of violence, stalking, defamatory content, and sending harmful messages. These actions are considered criminal offenses under various sections of Indian law, especially if they involve causing harm to the victim's reputation, mental well-being, or safety.

To sum it up, online harassment in India is addressed through various legal provisions that cover actions such as cyberbullying, identity theft, obscene content, defamation, and threats. Those who experience online abuse can report it to local authorities or use mechanisms under the IT Act for complaint.

CASE LAWS RELATING TO CYBER OFFENCES:

India has witnessed several landmark cyber law cases that have significantly shaped the legal landscape concerning cybercrimes, online defamation, and digital rights. One of the most pivotal cases is **Shreya Singhal v. Union of India (2015)**, where the Supreme Court struck down Section 66A of the Information Technology Act, 2000, deeming it unconstitutional for being vague and overbroad, thereby violating the right to freedom of speech and expression under Article 19(1)(a) of the Indian Constitution. This judgment reinforced the protection of online free speech in India.

Suhas Katti v. Tamil Nadu[1] is another noteworthy case; it was the first conviction in India for posting pornographic messages online under Section 67 of the Information Technology Act. An important step towards combating cybercrimes in India was taken when the accused was found guilty of sending offensive and defamatory messages in a Yahoo message group.

In **Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd. (2004[2])**, the Supreme Court held that domain names are akin to trademarks and that the Indian Trade Marks Act, 1999 applies to domain names. This decision emphasized the importance of protecting domain names under the law relating to passing off, thereby safeguarding brand identity in the digital space.

The case of **SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra (2001)** addressed cyber defamation through emails. The Delhi High Court issued an injunction against the defendant, restraining him from sending defamatory emails to the plaintiff, thereby recognizing cyber defamation as a legitimate cause for legal action in India.

[1] MHC, 2004.
[2] www.indiakannon.com

The Supreme Court decided in MouthShut.com v. Union of India[3] that intermediaries, such as social media platforms, cannot be held accountable for user-generated content unless they actually know it is unlawful. This ruling highlighted the necessity of striking a balance between online platforms' accountability and freedom of expression.

These cases collectively underscore the evolving nature of cyber laws in India, highlighting the judiciary's role in balancing technological advancements with the protection of individual rights and freedoms.

CONCLUSION

The gaps in legislation addressing online abuse and harassment in India are multifaceted, involving legal inadequacies, poor enforcement, gender insensitivity, and a lack of awareness. To effectively combat online abuse, India needs a more comprehensive and up-to-date legal framework that can address the complexities of digital harassment. This should include clearer guidelines for social media platforms, better training for law enforcement agencies, stronger penalties for offenders, and enhanced protections for vulnerable groups, especially women. In addition, a greater focus on public education, digital literacy, and data protection laws will help individuals better protect themselves and seek redress when they are targeted. Only through a concerted effort from lawmakers, technology companies, and civil society can India hope to reduce the prevalence of online abuse and harassment and ensure that its citizens can enjoy the benefits of digital spaces in safety and dignity.

References:

1. Cyber Law - B.M. Gandhi, 2nd edition.
2. Cyber Laws and practice- Bakshi- 2010.
3. Cyber law and IPR issues: the Indian perspective Mr. Atul Satwa Jaybhaye Bharati Law Review, April – June, 2016.
4. Commission on Intellectual Property Rights Study on Intellectual Property Rights, the Internet, and Copyright: Alan Story Lecturer in Intellectual Property Kent Law School, University of Kent.
5. Intellectual Property Rights And The Internet World Gunish Aggarwal Chandraprabhu Jain College of Higher Studies And School of Law, Narela, India
6. www.indiakannon.com
7. https://cag.gov.in/uploads/download_audit_report/2016/Chapter_7_Crime_Against_Women_Report_3_2016_Uttar_Pradesh.pdf
8. https://egyankosh.ac.in/bitstream/123456789/25925/1/Unit-13.pdf
9. www.unifem.org.in: UNIFEM South Asia homepage has links to UNIFEM resources and various activities currently going on in South Asia for women.
10. www.unfpa.org: UNFPA addresses VAWG and it's consequences particularly in reproductive health.

[3] SCC 2015