



JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1

Article 44

An Analysis of Legal Framework Governing Online Harassment

Jayanshu Raneja, BM Law College, Jodhpur

Recommended Citation:

Raneja (2026) “Legal Framework Governing Online Harassment” Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 44. (DOI)

This article is published under the Creative Commons Attribution–NonCommercial–ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows for free non-commercial use, distribution, and reproduction in any medium, provided appropriate credit is given to the original work.

INTRODUCTION

The rapid change in the Digital Communication platforms has changed the behaviour of people by bringing changes in the way of communication and expression of their thoughts and opinions. However, the development in the technology has invented various forms of online harassment which include cyberstalking, cyberbullying, trolling, identity theft, and doxing. Online harassment creates a serious threat to an individual's privacy, dignity, goodwill, and mental health. With the growth of the internet in India, our legal system has been facing challenges to address them.

This article evaluates the legal framework on online harassment in India, like its effectiveness, and identifies areas requiring improvement. It talks about the existing laws which provide a foundation for addressing cyber harassment, and difficulties in its enforcement.

UNDERSTANDING ONLINE HARASSMENT

The following acts are considered as Online harassment i.e. the act of scaring, threatening, verbally abusing, stalking, or humiliating individuals with the use of the Internet. Unlike traditional forms of harassment, online abuse can happen anonymously and spread rapidly, and remain accessible indefinitely. Victims have to face psychological distress, reputational damage, which may cause social isolation.

Common forms of online harassment include:

- Cyberstalking i.e. continues monitoring of someone.
- Cyberbullying which means targeting someone with abusive messages.
- Doxing means publishing someone's personal information without their consent.
- Impersonation and identity theft.
- Pornography for revenge and sharing someone's intimate images without any authority.

These are the types of harassment which are inter-connected to breach of privacy, defamation, and breach of personal safety of the individuals or victims.

STATUTORY FRAMEWORK GOVERNING ONLINE HARASSMENT

Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is an important legislative instrument which handles cybercrimes, as it has several provisions which are related to online abuse and harassment.

Section 66C of this Act, Identity theft means fraudulently using another person's electronic or digital signature, password, or unique identification feature is considered as an offense. Section 66D talks about the punishment for fraud committed by impersonating another person using computer resources; these provisions are particularly applicable when offenders create fake profiles or impersonate themselves as victims¹.

Section 67 prohibits the publication or transmission of obscene material in electronic form, while Sections 67A and 67B provide for very strict penalties regarding sexually explicit material and material related to the sexual exploitation of children².

Although these provisions address specific forms of cyber abuse, the IT Act does not give a detailed definition of online harassment.

Bhartiya Nyaya Sanhita, 2023

The Bhartiya Nyaya Sanhita (BNS) which has been replaced with the Indian Penal Code (IPC), provides provisions about online abuse for which legal action can be taken for the offences like threats, criminal intimidation, defamation, stalking, obscenity, and crimes against women committed through electronic machines.

There is a provision regarding the offense of 'stalking' which is significant for addressing persistent online surveillance and unwanted contact. Similarly, provisions related to criminal intimidation can be invoked against individuals who give threats through social media platforms like WhatsApp, Instagram, Telegram applications, or email etc³.

¹ Information Technology Act, 2000: The IT Act, 2000, Act No. 21 of 2000 (India)

² MINISTRY OF ELEC. & INFO. TECH., GOV'T OF INDIA, meity.gov.in [perma.cc](accessed on June 25, 2026)

³ Bhartiya Nyaya Sanhita, 2023: The Bhartiya Nyaya Sanhita, 2023, Act No. 45 of 2023 (India)

PROTECTION OF WOMEN'S RIGHTS IN CYBERSPACE

The most affected class of the society from online harassment are the women. Acts such as the sharing of private images without consent, sending sexually offensive messages, and stalking frequently by targeting women and girls.

Our legal system wants to address such behavior under the IT Act and criminal laws. The Courts have recognized these acts as digital harassment which is a violation of dignity, privacy, and personal liberty of the victims. The Supreme Court's recognition of privacy as a fundamental right has given more strength to the legal protection for the victims⁴.

JUDICIAL APPROACH TOWARDS ONLINE HARASSMENT

Indian courts are acting as an important pillar for protecting individuals from online harassment or abuse and the freedom of expression of the people.

In the case of *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the Information Technology Act on the grounds that it imposes unreasonable restrictions on freedom of speech. While this judgment strengthened the constitutional safeguards for online expression, it also said about the need for precise laws that should focus on actual instances of cyber-harassment rather than just imposing restrictions on speech.

Courts have also actively acknowledged the seriousness of issues such as cyber-stalking, online threats, and the non-consensual sharing of private information. Judicial rulings tell us that the harm done by the virtual offences also imposes harm to the actual world⁵.

CHALLENGES IN ENFORCEMENT

Absence of a Comprehensive Legal Definition

The absence of a uniform legal definition of online harassment is a major challenge. The provisions which tell about various forms of abuse are scattered across multiple different laws. This difference in the law creates an uncertainty for the law enforcement agency and the courts.

⁴ JUSTICE YATINDRA SINGH, CYBER LAWS (Universal Law Publishing)

⁵ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1

Jurisdictional Difficulties

Digital communications are often beyond geographical boundaries. A criminal operating from another state or country can target anyone in the world. Such offences done cross-border create difficulty for investigation, evidence collection, and prosecution because of lack of jurisdiction.

Anonymity and Technological Barriers

Due to the internet, it's very easy for the criminals to hide their identities by using anonymous accounts, virtual private networks, and encrypted services due to which the Law enforcement agencies have to face technical challenges in tracking those criminals and securing digital evidence⁶.

Underreporting

Many victims avoid reporting these kinds of incidents due to fear, social stigma, or a lack of faith in the legal system as they fear that their reputation will be damaged in the society if they will report about the abuse. Women, minors, and marginalized groups are particularly prone to facing such barriers.

CRITICAL EVALUATION AND REFORM PROPOSALS

Although India has various legal provisions for cyber harassment, the current system largely acts only after an incident has occurred. There is a need for a victim centric approach, we should not wait for an offence to happen and then take action on that, we should be aware about the safety measures for dealing with these kinds of incidents.

Firstly, the Parliament should formulate a legal definition for online harassment that includes cyberstalking, cyberbullying, doxing, and similar forms of harassment. These kinds of legislations will bring clarity about these offences and will remove the uncertainty for the law enforcement agency regarding the provisions which tells about various forms of abuse across multiple different laws⁷.

⁶ NAT'L CYBER CRIME REPORTING PORTAL, cybercrime.gov.in [perma.cc](accessed on June 25, 2026)

⁷ APAR GUPTA, COMMENTARY ON INFORMATION TECHNOLOGY LAW (LexisNexis)

Second, special cybercrime units should be formed and shall receive better technical training and resources which will help in effective investigation of digital crimes and stopping them from happening in future.

Third, social media platforms shall adopt improved reporting systems which collaborate more efficiently with the law enforcement agencies and cyber cell through which they can report the offence to the agencies for fast action, while respecting privacy and legal procedures.

Fourth, every citizen should be aware and educated about digital safety, how to report, and what are the legal remedies for them, through public awareness campaigns so that they do not get harassed by anyone and even if something happens they will have complete knowledge about what steps they have to take for it.

Finally the victims of online harassment should be provided with greater support services, such as counseling and legal assistance which will help them to overcome the abuse and will also encourage other victims to report about the offence which has happened with them so that the law enforcement agencies can take action for them.

CONCLUSION

In this digital age online harassment is one of the biggest legal and social concerns. India's current laws such as the Information Technology Act, 2000, and the Bhartiya Nyaya Sanhita, 2023 provide necessary measures to address different forms of cyber abuse. But, the lack of a comprehensive legal framework, with implementation challenges and technical complexities, puts a barrier in the current effectiveness safeguards and as a result these kinds of offences keep increasing day by day and mostly women and girls are the one who have to suffer from these offences.

As with the transformation of modern communication through digital platforms, the laws should be evolved for protecting individuals from online abuse while upholding the constitutional freedom, for e.g. as everyone should have a right to speak but they should be in their limit so that the other person do not feel harassed. Creating a safe digital environment which has a balanced approach that integrates legal reforms, effective enforcement, and public awareness.