

Digital Spaces, Systemic Harms: Evaluating Legal Frameworks and Protective Mechanisms for Vulnerable Groups under the Indian Legal System

Soma Gupta¹, Dr.Pushpendra Singh²

^{1,2}Assistant Professor, Govt Law College, Tikamgarh M.P

Abstract

The digital landscape has evolved into an omnipresent infrastructure that basically shapes modern human communication, commerces, business and entertainment. Nonetheless, this speedy expansion has resulted in sharp escalation in cyber-violence, transforming online platforms as systemic harm that directly threaten human rights, dignity mental well-being, good will and public images . While digital spaces offer unparalleled connectivity, they also arbitrarily expose specific vulnerable demographics most notably women, minors, and historically marginalized communities to targeted abuse. Addressing this urgent crisis requires examining cyber-violence.

To address these challenges, this paper presents a detailed examination of the modern digital safety crisis, beginning with a comprehensive typology of online harassment that categorizes forms of harm ranging from verbal abuse and cyber stalking and AI-generated deepfakes. Building on this classification, the research analyzes the heightened risks faced by marginalized populations through an intersectional framework, illustrating how overlapping identity factors exacerbate individual vulnerability. The study further assesses the real-world consequences of these behaviors, detailing the severe psychological trauma, economic hardship, and digital exclusion experienced by victims. Finally, by evaluating the structural limitations of existing legal frameworks, law enforcement capabilities, and platform-level content moderation, this paper advances a synchronized, three-tiered solution combining international legal reform, Safety-by-Design technological architecture, and widespread digital citizenship education to cultivate a safer, more equitable online ecosystem.

Introduction

Online harassment can be defined as the use of the web world or the digital platforms where any digital form of communication is used to exchange the information by one person or a group of person to harass, harm, intermediate or defame any other person or a group of persons This may involve intimidations, humiliation, or mortification in an online setting. This comprises expressions of prejudiced attitudes and beliefs, such as sexism, racism, nationalism, homophobia, transphobia, religious extremism, hate speech ,online sexual harassment, cyberstalking, and image based sexual abuse or other unwanted online conduct of a sexual nature It takes place in contexts such as social media (Facebook, Instagram, Snapchat, TikTok, and Twitter), SMS, instant messaging (via devices, email provider services, apps, and social media messaging features) . Cyberbullying in the Indian context is a complex

and evolving challenge that requires a nuanced legal response. This case study has explored the prevalence and impact of cyberbullying, the existing legal framework, landmark cases, and the challenges associated with prosecuting offenders. While legal remedies are available, the effective implementation of these measures necessitates a collaborative effort involving government agencies, legal professionals, NGOs, and the public. As technology continues to advance, policymakers and legal practitioners must remain vigilant in adapting legal frameworks to address emerging threats in the digital landscape.

Understanding the concept and Definition of cyber-violence / harassment and the evolution of the digital landscape.

Cyber harassment is not defined as a single standalone phrase in Indian statutes, but Indian law addresses it through provisions covering electronic obscenity, invasion of privacy, and cyber stalking. This includes a wide range of harmful activities committed through electronic communication, messaging applications social media platforms and other digital means. *It includes cyber stalking, online harassment, cyber bullying, identity theft, defamation, and the non-consensual distribution of explicit content*

Cyber-harassment, also referred to as online harassment or online abuse, refers to a situation in which an individual or group is severely or pervasively targeted through harmful online behaviour that may be for either a short or extended duration, may be perpetrated by either an individual or coordinated by a group of people, and which is aimed at causing severe emotional distress or emotional harm¹

Cyber violence being a relatively new phenomenon that encompasses a wide variety of crimes, the term is still difficult to define precisely. Commonly it can be defined as:

“The use of computer systems to cause, facilitate, or threaten violence against individuals, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristics or vulnerabilities.”²

Cyber-violence and digital harassment encompass a spectrum of unlawful, non-consensual, and abusive conduct perpetrated through Information and Communication Technologies (ICT) such as mobile devices, computers, and social media platforms, they are specifically designed to inflict severe emotional, psychological, or physical distress upon a victim. *A primary driver of this phenomenon is the perceived anonymity afforded by digital environments, where perpetrators frequently employ pseudonymous accounts, fraudulent identities, or unauthorized access to obscure their real-world identities and evade accountability.* As a consequence, victims frequently suffer from acute psychological trauma, including severe anxiety, depression, and profound social isolation. Crucially, these digital offenses rarely remain confined to virtual spaces, as online threats routinely cross over into real-world physical danger, offline stalking, and direct safety risks.

This form of technology-facilitated abuse manifests through several distinct, legally recognized offenses that undermine bodily autonomy, privacy, and personal security. Cyberstalking involves a continuous, willful course of conduct marked by persistent unwanted electronic communications, unauthorized digital surveillance, and tracking designed to instil fear and impair a person's sense of safety. Simultaneously, bad actors frequently engage in doxxing—the malicious, unauthorized dissemination of

¹ Media Defence, ‘Factsheet: Gender and Online Harassment’ (2021) (accessible at <https://www.mediadefence.org/resource-hub/resources/gender-online-harassment-factsheet>).

² <https://www.coe.int/en/web/cyberviolence>

Personally Identifiable Information (PII) such as residential addresses, phone numbers, or place of employment—with the explicit intent to incite third-party harassment or physical harm.

Furthermore, digital abuse often intersects with criminal privacy violations through Non-Consensual Intimate Image (NCII) distribution, commonly referred to as image-based sexual abuse. This occurs when an individual unlawfully publishes, shares, or threatens to expose sexually explicit photos or videos without consent, frequently serving as an instrument for extortive blackmail, extortion, or public humiliation. Finally, systemic online abuse is amplified through targeted trolling and hate speech, which constitute severe verbal harassment and incitement to violence aimed at individuals based on protected characteristics such as race, gender, religion, or sexual orientation. Together, these actions constitute severe legal violations encompassing criminal intimidation, defamation, and gross privacy infringement. Cyber-harassment can occur in a variety of forms that specifically target women and might be considered an umbrella term for a range of other digital attacks, such as

- **Cyber bullying**, which is common among children and young adults and typically involves sending digital messages that are aimed at causing embarrassment or humiliation

Cyber bullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyber bullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. It includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyber bullying crosses the line into unlawful or criminal behaviour.³

The most common places where cyber bullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities
- **Non-consensual dissemination of intimate images** which refers to the sharing or publication of images of a subject, whether obtained with or without consent, with the aim of causing them harm. Non-consensual dissemination of intimate images (NCDII) is a form of image based sexual abuse (IBSA) which involves the sharing of intimate sexual images of another person without their consent. Despite the impact that this form of NCDII has on victims, including shame, humiliation, PTSD, anxiety, depression, and suicide, little is known about the psychological mechanisms that may promote this behaviour.⁴
- **Online sexual harassment**, which refers to exposing a subject to unwanted direct or indirect, verbal, or non-verbal content of a sexual nature, such as the unsolicited sending and or receiving of sexually explicit material that violates the dignity of a person and creates a hostile or humiliating environment. Online sexual harassment is any unwanted sexual behaviour online. It can make a person feel threatened, exploited, coerced, humiliated, upset, sexualised or discriminated against.

³ <https://www.stopbullying.gov/cyberbullying/what-is-it> last seen on 13th Aug 2026

⁴ https://www.researchgate.net/publication/392434166_Non-consensual_Dissemination_of_Intimate_Images_The_Roles_of_Dark_Personality_Traits_and_Online_Disinhibition_Dissemination_Proclivity_and_Attitudes

- **Hate speech**, whether through social media posts or digital mail, which is targeted at one's actual or presumed protected characteristics, such as gender, sexuality, or race, including the use of sexist or gendered name-calling.
- **Online sexual exploitation** which refers to the use of digital technologies to exploit or abuse a position of power over a victim for sexual purposes. It occurs in many forms including online grooming, live streaming of sexual abuse, child sexual abuse material (CSAM), online sex trafficking, online sexual coercion, and image-based sexual abuse. While these types of violations are not new, digital technologies have provided a platform through which perpetrators can reach wider audiences and derive illicit financial gain. This form of violence disproportionately affects women and children.

2. How is Criminal Liability Is Established in Cyber Harassment Cases

The legal framework addressing cyberbullying in India comprises a combination of statutes and judicial decisions.

The Information Technology Act of 2000 was originally intended to offer legal recognition for electronic commerce and promote the expansion of the internet in India. However, as online crimes like cyber bullying became increasingly common, the IT Act was updated to handle these new concerns.

- **The following main sections of the IT Act address cyber bullying:**

- a. Section 66A: Sending Offensive Messages (Prior to Repeal)**

Section 66A of the IT Act, which was created to address offensive internet messages, was a critical element for combating cyberbullying. It prohibited the transmission of insulting or menacing messages via communication services, social media, or email. This area was frequently used in cases when people were harassed or intimidated online.

However, in 2015, the Supreme Court of India declared Section 66A unconstitutional because it was extremely ambiguous and restricted freedom of speech and expression under Article 19(1)(a) of the Indian Constitution. Despite being repealed, this clause had a considerable impact on the approach to cyberbullying laws in India.

- b. Section 66C: Identity Theft and Impersonation**

Section 66C of the IT Act makes it illegal to perpetrate identity theft or impersonate someone online. This is especially true in cases of cyberbullying, in which people create phony identities or mimic others in order to destroy their reputation or harass them. This clause penalizes identity theft with up to 3 years of imprisonment and a fine of up to ₹1 lakh.

- c. Section 66E: Violation of Privacy**

The violation of privacy clause (Section 66E) makes it illegal to capture, publish, or transmit intimate or private photos of another person without their permission. Cyberbullies frequently publish private or embarrassing images to humiliate or shame victims, making this part of the IT Act extremely relevant to instances of cyber bullying.

- d. Section 67: Punishment for Obscene Content**

Section 67 addresses the publication or transmission of obscene content via electronic means. It is primarily aimed at the online publication of obscene material and has been utilized in cases of cyberbullying where harmful, graphic, or libelous content is posted to frighten or harass people.

- **The Bharatiya Nyaya Sanhita, BNS**

In addition to the IT Act, the Bharatiya Nyaya Sanhita (BNS) provides legal remedies for cyberbullying-

related offenses. The BNS has several laws that can be used to address situations of internet harassment, stalking, and defamation.

a. Section 356 (1) – Defamation: Defamation occurs when someone makes false and damaging claims about another person with the intent to hurt their reputation. Defamation in cyberbullying frequently takes the form of spreading false rumors, uploading harmful content, or revealing embarrassing facts. Such crimes are criminalized under BNS Section 356 (1), with penalties ranging from imprisonment to fines.

b. Section 351 (2)/(3) – Criminal Intimidation: Threatening someone with injury or harm is a criminal offense under Section 351 (2)/(3) of the BNS. Criminal intimidation in cyberbullying frequently takes the form of online threats delivered via messages, emails, or social media platforms. This clause empowers cyberbullying victims to seek judicial redress when threats are made against them.

c. Section 78 – Stalking: Cyberstalking is a severe type of cyberbullying, and Section 78 of the BNS expressly targets it. The clause criminalizes stalking, including internet stalking, which is the act of continuously observing a person's online activity, sending unsolicited communications, or participating in behavior that intrudes on the victim's privacy. Cyberbullies frequently use online stalking to frighten and torment their victims.

d. Section 351 (4) – Criminal Intimidation by Anonymous Communication: Section 351 (4) of the BNS makes it illegal to threaten someone through anonymous communication. In many situations of cyberbullying, the attacker conceals their identity, making it difficult for the victim to pursue justice. This provision addresses the issue and provides for prosecution, even if the bully remains nameless.

- **Juvenile Justice (Care and Protection of Children) Act, 2015**

Cyberbullying involving kids, whether as victims or perpetrators, is addressed by the Juvenile Justice (Care and Protection of Children) Act of 2015. The statute requires the protection of children against abuse, exploitation, and dangerous online content. It also offers rehabilitation and counseling to adolescents who engage in cyber bullying. Rather than focusing exclusively on punishment, the law prioritizes reform and rehabilitation for juvenile offenders.

- **Landmark Cases:**

Several landmark cases in India have contributed to the evolving jurisprudence on cyberbullying. The 2015 case of *Shreya Singhal v. Union of India* marked a watershed moment, with the Supreme Court striking down Section 66A of the IT Act. The judgment affirmed the importance of protecting free speech while acknowledging the need for a nuanced legal approach to cybercrimes. Subsequent cases, such as *Rajat Prasad v. CBI* (2014) and *R v. Juggernaut Books Pvt Ltd* (2018), have provided guidance on issues related to online harassment and defamation.

The case of *Rini Johar v. State of MP* (2019) is noteworthy for addressing cyberbullying within the context of workplace harassment. The court recognized the severity of online abuse and affirmed that existing legal provisions could be applied to combat cyber bullying in employment settings.

Legal Remedies and Support Systems:

Victims of cyber bullying in India can avail themselves of various legal remedies and support systems. Reporting cyber bullying incidents to law enforcement agencies, such as the Cyber Crime Cells established in many cities, is a crucial initial step. The National Cyber Crime Reporting Portal, launched by the Ministry of Home Affairs, provides an online platform for reporting cybercrimes, including cyber bullying.

The Cyber Crime Punishment in India varies according to the precise statutes under which the perpetrator is charged. These **cyber bullying penalties** typically involve fines, incarceration, or both.

a. Imprisonment and fines: Offenders found guilty of cyber bullying under sections 66C (identity theft), 66E (privacy violations), and 67 (obscene content) risk jail sentences ranging from one to five years, depending on the gravity of the offense. The punishments for these infractions can range from ₹1 lakh to ₹5 lakh.

More serious acts, such as stalking or criminal intimidation, can result in harsher punishments, including longer jail sentences and larger fines.

b. Non-Bailable Offenses: Certain cyberbullying charges, such as child pornography or cyberstalking, are considered non-bailable. This means that the accused will not be granted bail quickly and would have to go through a more rigorous legal process.

c. Compensation for Victims: In addition to jail or penalties, victims of cyberbullying in India may seek restitution for the harm done. The courts may order the offender to compensate the victim for mental suffering, reputational damage, or financial losses resulting from the bullying. This is a sort of restitution for the victim's suffering.

d. Rehabilitation of Minors: For minors who engage in cyberbullying, the legislation promotes rehabilitation above punishment. Minors who engage in cyberbullying may be required by the Juvenile Justice Act to receive counseling, participate in awareness programs, or perform community service.

Challenges in Prosecuting Cyber bullying:

Despite the existing legal framework, prosecuting cyber bullying cases in India presents numerous challenges. The anonymous nature of online platforms often complicates the identification and apprehension of offenders. Additionally, the lack of awareness about legal remedies and the stigma associated with being a victim of cyber bullying contribute to underreporting.

The dynamic and borderless nature of the internet further poses challenges in enforcing judgments, especially when perpetrators and victims are located in different jurisdictions. The need for international cooperation and mutual legal assistance is underscored in cases involving cross-border cyberbullying.

Addressing the complex issue of cyberbullying in India requires a comprehensive and multifaceted approach. Policymakers should consider:

- **Legislative Amendments:** Regular review and amendment of existing laws to keep pace with technological advancements and emerging forms of cyberbullying.
- **Awareness Campaigns:** Targeted campaigns to educate individuals, schools, and workplaces about the consequences of cyberbullying and the available legal remedies.
- **International Collaboration:** Strengthening collaborations with international law enforcement agencies to address cross-border cyberbullying cases effectively.
- **Capacity Building:** Enhancing the capabilities of law enforcement agencies, legal professionals, and the judiciary to investigate and adjudicate cyberbullying cases.
- **Research and Data Collection:** Ongoing research to understand the evolving nature of cyberbullying, its impact on diverse populations, and the effectiveness of legal interventions.

Recommendations

To move from reactive litigation to proactive prevention, the legal, technological, and institutional frameworks governing technology-facilitated abuse must be systematically modernized:

a. Statutory Clarification on AI and Synthetic Media

While the **Bharatiya Nyaya Sanhita (BNS), 2023** updated criminal provisions like Section 78 (Stalking) and Section 351 (Criminal Intimidation), it does not explicitly define AI-generated synthetic harm or deepfakes. Legislation must be enacted or updated to:

- Explicitly criminalize the **non-consensual creation and dissemination of synthetic intimate imagery** (deepfake NCII) regardless of whether financial extortion was intended.
- Mandate **digital watermarking and cryptographic provenance metadata** for generative AI developer models operating within Indian jurisdiction.

b. Operationalizing Intermediary Compliance & "Safety-by-Design"

The implementation of Rule 3(2)(b) of the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** requires stricter enforcement:

- **Perceptual Hashing Infrastructure:** Platforms must be required to integrate centralized, privacy-preserving hash repositories (such as the I4C Sahyog Portal hash bank) to instantly block the re-uploading of reported intimate images.
- **Proactive Content Audits:** Platforms should deploy automated crawler technologies to identify viral harassment campaigns before they result in irreparable reputational and psychological harm to victims.

c. Judicial Capacity & Specialized Evidence Handling

- **Evidentiary Streamlining:** Judicial and law enforcement personnel need targeted training on the procedural mandates of the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, particularly regarding the electronic evidence chain of custody (Section 63B) in cross-border metadata requests.
- **Fast-Track Cyber Tribunals:** Designate specialized magistrate benches for fast-tracking emergency takedown orders and protection mandates in cyberstalking and doxxing cases.

Conclusion

Cyber-violence and technology-facilitated harassment represent a growing threat to fundamental constitutional rights in the digital age. By targeting bodily autonomy, privacy, and freedom of expression, online abuse disproportionately restricts the digital participation of women, minors, and historically marginalized communities.

While the transition from the Indian Penal Code to the **Bharatiya Nyaya Sanhita, 2023**—complemented by the IT Act, 2000 and the IT Intermediary Rules, 2021—provides an updated legal foundation, enforcement challenges persist due to platform anonymity, jurisdictional boundaries, and rapid technological advancements like generative AI. Transforming digital spaces into safe environments requires a synchronized approach combining precise statutory updates, platform accountability, specialized law enforcement capabilities, and institutional digital citizenship education. Ensuring safety in cyberspace is not merely a matter of regulation, but a constitutional imperative to preserve human dignity and equal opportunity for all.

References and endnotes

1. **Bharatiya Nyaya Sanhita, 2023.** (Act No. 45 of 2023). Universal Law Publishing / Government of India.
2. **Bharatiya Sakshya Adhiniyam, 2023.** (Act No. 47 of 2023). Government of India.

3. **Information Technology Act, 2000.** (Act No. 21 of 2000). Bare Act with Short Notes. Commercial Law Publishers.
4. **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.** Ministry of Electronics and Information Technology (MeitY), Government of India.
5. **Ministry of Electronics and Information Technology (MeitY).** (2025). *Standard Operating Procedure (SoP) for the Removal and Prevention of Non-Consensual Intimate Imagery (NCII) Content.* Government of India.
6. **Henry, N., & Powell, A.** (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, & Abuse*, 19(2), 195–208.
7. **Media Defence.** (2021). *Factsheet: Gender and Online Harassment.* Media Legal Defence Initiative.
8. **Shreya Singhal v. Union of India**, (2015) 5 SCC 1 (Supreme Court of India).
9. **Rini Johar v. State of Madhya Pradesh**, (2016) 11 SCC 703 (Supreme Court of India).
10. **Council of Europe.** (2020). *Cyberviolence Against Women and Girls: Key Concepts and Definitions.* Cybercrime Division, CoE.

Endnotes

1. Media Defence, *Factsheet: Gender and Online Harassment* (2021), available at: <https://www.mediadefence.org/resource-hub/resources/gender-online-harassment-factsheet> (last visited Aug. 12, 2026).
2. Cybercrime Division, Council of Europe, *Cyberviolence Concepts and Definitions* (2020), available at: <https://www.coe.int/en/web/cyberviolence> (last visited Aug. 12, 2026).
3. StopBullying.gov, *What is Cyberbullying* (U.S. Department of Health and Human Services, 2021), available at: <https://www.stopbullying.gov/cyberbullying/what-is-it> (last visited Aug. 13, 2026).
4. Nicola Henry and Anastasia Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research" 19(2) *Trauma, Violence, & Abuse* 195–208 (2018).
5. Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66E, 67, 67A.
6. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
7. Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 78, 351, 356.
8. Juvenile Justice (Care and Protection of Children) Act, 2015 (Act 2 of 2016).
9. *Rajat Prasad v. CBI*, (2014) 6 SCC 495; *Rini Johar v. State of Madhya Pradesh*, (2016) 11 SCC 703.
10. Ministry of Home Affairs, Government of India, *National Cyber Crime Reporting Portal*, available at: <https://cybercrime.gov.in/> (last visited Aug. 13, 2026).
11. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(2)(b).
12. Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
13. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63B.
14. Protection of Children from Sexual Offences (POCSO) Act, 2012 (Act 32 of 2012).
15. Communications Decency Act, 1996, 47 U.S.C. § 230 (United States).
16. Online Safety Act, 2023, c. 50 (United Kingdom).
17. Enhancing Online Safety Act, 2015 (Australia).
18. Protecting Canadians from Online Crime Act, S.C. 2014, c. 31 (Bill C-13, Canada).