INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

CYBERSTALKING AND CYBERBULLYING IN THE DIGITAL AGE: LEGAL FRAMEWORK AND SOCIETAL IMPLICATIONS IN INDIA

[1]Shahil Rangra, [2]Monika Rangra
[1]Research Scholar, [2]Assistant Professor
[1]Department of Law,
[1] Himachal Pradesh University, Summer Hill Shimla, 171005, India

Abstract : The use of digital platforms has revolutionized the way humans interact, but it has also given rise to dangerous online behaviour like cyberbullying and cyberstalking. These activities, usually conducted in the cloak of anonymity, have the potential to cause serious psychological damage to people, leading to emotional trauma, social isolation, and in extreme cases, even self-inflicted harm or suicide. Cyberstalking is characterized by repeated and intrusive behaviour such as monitoring, threats, or unwanted contact via electronic means. Cyberbullying, however, generally targets adolescents and involves harassment, defamation, or public humiliation through social media, messaging platforms, and other online forums. Within India, although certain advances have been made in penalizing cyberstalking—through provisions in the Bharatiya Nyaya Sanhita, 2023 (BNS)(e.g., Section 78) and the Information Technology Act—cyberbullying is too poorly defined under the law. This lack of a clear definition in legislation makes it harder to prosecute and limits the protection of victims, notably children and women. The current statutory law and milestone court rulings on cyberstalking and cyberbullying have been critically assessed in this paper. It further emphasizes the implications of advances in technology, e.g., the changing means of abuse on the internet and challenges in tracking perpetrators who hide their identities. Besides the legal aspects, the research has taken into account the larger social implication of these crimes, such as how they impact mental well-being and online security. The article ends with proposals directed towards legal reform, improved enforcement mechanisms, online education, and the establishment of support networks for victims.

Keywords: Cyberbullying, Cyberstalking, Digital Harassment, Indian Legal Framework, Online Safety

1. Introduction

In the digitally connected world of today, the internet has become an integral part of everyday life, revolutionizing the way people communicate, socialize, work, and access information. Social media sites, messaging apps, and other online forums provide unparalleled opportunities for interaction and self-expression. But with these advantages come the drawbacks of the digital world as well—most significantly, cyberstalking and cyberbullying. These crimes take advantage of the far-reaching extent and comparative anonymity of the internet so that offenders can harass victims with little risk of discovery or repercussions. Cyberstalking is the repeated application of electronic communication to harass, monitor, or threaten a victim. This could involve sending persistent messages, tracking online behaviour, impersonation, or even breaking into personal accounts. Cyberbullying, although in its intent to cause harm similar to that of stalking, tends to happen among teenagers and is characterized by spreading rumours, posting embarrassing content, or engaging in online exclusion or defamation. Both offenses are highly invasive and can have long-term psychological impacts on victims, such as anxiety, depression, social isolation, and in extreme cases, suicidal thoughts or self-injury.[1]

In India, cyberstalking has evolved incrementally into legal recognition, specifically by the addition of Section 78 in the Bharatiya Nyaya Sanhita, 2023 (BNS)and some provisions of the Information Technology Act, 2000. Cyberbullying, on the other hand, is a grey area within the legal framework, as there is no explicit statutory definition and no special law to tackle it effectively. This vacuum in law is highly challenging for victims in pursuit of justice and indicates an immediate need for legislative change.[2]

This paper seeks to examine the nature and extent of cyberstalking and cyberbullying in India, evaluate the efficacy of existing legal provisions, and analyse the social implications of these digital crimes. It also makes suggestions for making the laws more effective, raising the level of public awareness, and improving support systems to safeguard victims in the fast-evolving digital era.

Cyberbullying in India is carried out in different detrimental forms, each with the potential to cause deep emotional and psychological harm.[3] Common forms include cyberstalking, in which the abuser continuously monitors and harasses the victim online using threats or fabrications. Social cyberbullying involves circulating hurtful rumours or embarrassing content on social media platforms to tarnish an individual's image or reputation.[4] Exclusion, or cyber ostracism, involves the intentional exclusion of an individual from online interactions, which can have a detrimental effect on mental health.[5] Revenge porn, or non-consensual pornography, involves the unauthorized distribution of intimate images or videos, often as a weapon of humiliation or blackmail.[6] Trolling is the practice of inciting users by using offensive or inflammatory comments to cause emotional distress. Impersonation entails the construction of fictitious identities or the misuse of another person's personal information for the purpose of disseminating misinformation or inflicting reputational damage.[7] Lastly, trickery constitutes deceptions in which a bully manipulates a victim to gain his or her trust before breaking such trust by revealing sensitive information. These various types of cyberbullying underscore the necessity of effective awareness campaigns, prevention measures, and legal protection.[8]

2. Legal Provisions Pertaining to Cyberstalking and Cyberbullying:

Cyberstalking is specifically dealt with under **Section 78 of the Bharatiya Nyaya Sanhita, 2023 (BNS)**, which was enacted by way of the corresponding to the erstwhile Section 354D of the Indian Penal Code, 1860. The provision criminalizes it when a man stalks or tries to make contact with a woman in spite of her clear disinterest. More particularly, the law criminalizes repeated efforts to contact a woman by physical or electronic means, such as email, social media, or other digital means, with the purpose of pursuing or intimidating her. It also covers tracking her online activities without her consent. The provision recognizes the intrusive and ongoing nature of such behaviour, which can greatly erode a woman's feeling of safety and privacy.

Conversely, cyberbullying in India is still a comparatively undefined and poorly regulated phenomenon in the legislative legal framework. Even though it is not directly codified within any particular section of Indian law, cyberbullying typically entails repeated application of online communication for the purpose of harassing, insulting, or psychically tormenting a person. This can include activities such as spreading false rumours, posting embarrassing pictures or videos, sending threatening messages, or online ostracism. The action is usually meant to damage the victim's reputation, self-esteem, or emotional health.

Although there is no formal definition, some provisions of the Information Technology Act, 2000 and other sections of the BNS can be used to deal with acts of cyberbullying, depending on the severity and nature of the offense. Yet, the absence of a clear legal categorization makes enforcement uncertain and impedes uniform legal recourse for victims, particularly children and vulnerable adults.[9]

In addition, the Digital Personal Data Protection Act, 2023 introduces a comprehensive framework for the protection of personal data in India. The Act is particularly relevant in the context of cyberstalking and cyberbullying, where misuse of personal information, unauthorized sharing of images, and digital surveillance are common. By regulating the collection, processing, and dissemination of personal data, the Act strengthens privacy safeguards and provides a preventive dimension to addressing online harassment.[10]

2.1. Legal Provisions Pertaining to Cyberstalking:

Section 78, Bharatiya Nyaya Sanhita, 2023 (BNS): Criminalizes cyberstalking specifically.

- Applies when a man continues to follow or contact a woman even after she has made it clear that she is not interested.
- Encompasses actions like sending messages, emails, or monitoring online activities without permission.
- Punishable by imprisonment, which can be up to three years for the first conviction and five years for repeat offenses, and also a fine.

2.2. Legal Provisions Governing Cyberbullying (Not specifically addressed, but falling under other laws):

- Section 356, BNS – Defamation:

Applicable when false and defamatory content is put online to defame a person. Can be applied in online character assassination or public humiliation cases.

- Section 357, BNS – Punishment for Defamation:

Imposes punishment for defamation, including cyber defamation, in the form of imprisonment for up to two years, fine, or both.

- Section 351(2), BNS – Criminal Intimidation by Anonymous Communication:

Deals with threats or harassment communicated anonymously through digital means like spoofed emails or social media profiles.

- Section 66C, IT Act, 2000 – Identity Theft:

Punishes the use of another person's personal information (such as photos or login credentials) to impersonate or harass them online.

- Section 66D, IT Act – Cheating by Personation Using Computer Resource:

Used when people impersonate others online to harass, humiliate, or deceive.

- Section 67, IT Act – Publication of Objectionable Content in Electronic Form:

Addresses distribution of sexually explicit or offensive material to harass or embarrass someone online.

- Protection of Children from Sexual Offences (POCSO) Act, 2012:

Used when cyberbullying contains minors, particularly sexual harassment or encountering obscene content online.[11].

3. Landmark Cases

3.1. Vishakha v. State of Rajasthan, (1997) 6 SCC 241

Though not specifically a case of cybercrimes, this historic ruling set the precedent for dealing with sexual harassment in India. The Supreme Court laid down the Vishakha Guidelines, which set out the definition of sexual harassment and established guidelines for its prevention in the workplace. These directives subsequently impacted legal comprehension of harassment on the internet, where women experience similar kinds of abuse, including unwanted messages, threats, and stalking on online platforms. The case stressed safeguarding the dignity, privacy, and safety of women, which is echoed in comprehension of laws regarding online harassment.[12]

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

This landmark judgment struck down Section 66A of the Information Technology Act, 2000 on the ground that it violated the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution. The Court held that vague and overbroad restrictions on online speech could lead to misuse and arbitrary enforcement. This case is highly relevant in the context of cyberbullying, as it highlights the challenge of balancing regulation of harmful online content with protection of free speech.[13]

3.3. Ritu Kohli Case (2001)

Extensively considered to be India's first reported case of cyberstalking. The accused pretended to be Ritu Kohli on the internet chat forums, providing her personal details and interacting with strangers on obscene topics using her name. The case highlighted the need for speedy legal changes to deal with technology-facilitated crimes. It was also one of the first times the Information Technology Act, 2000, had been used by the police. It acted as a wake-up call to the abuse of anonymity and internet communication for stalking and harassment.[14]

3.4. Ritika Sharma Case

The case focused public minds on the psychological and emotional burden that cyberbullying can put on victims, particularly young women. It pointed to the importance of prompt and sensitive police response, not merely to punish the perpetrator but to also provide for the timely provision of emotional and psychological support to the victim. The case highlighted that psychological trauma should be addressed as an essential outcome of cybercrimes deserving both legal remedies and counselling or rehabilitation assistance for the victim.[15]

3.5. Shibani Barik v. State of Odisha (2020)

Facts of the Case: In this landmark 2020 case, the petitioner Shibani Barik was charged with abetting the suicide of her husband. The charges indicated that she was having an extramarital affair and had allowed her co-accused to share intimate videos of herself with the said person on a public social media platform, i.e., TikTok. These videos allegedly led to extreme emotional distress to her husband, eventually causing him to commit suicide. Charges were filed under Section 108 of the Bharatiya Nyaya Sanhita, 2023 (BNS) after the incident, which deals with abetment of suicide. The case was argued before the Orissa High Court, and the bail application was heard under Section 483 of the Bharatiya Nagarik Suraksha Sanhita, 2023.

Judicial Observations and Findings: In granting the accused bail, the High Court made a few significant observations. The court was alarmed at the increasing abuse of social media sites such as TikTok, which the court pointed out were being used more and more to post objectionable, abusive, and offensive content. The judgment recognized that this content could significantly affect a person's mental health, and in the worst possible cases, result in psychological collapses or suicide, as in this case was allegedly the case.

Notably, the court highlighted the insufficient nature of cyber laws in dealing with such contemporary digital threats. It noted that although pieces of legislation such as the Information Technology Act, 2000, are in place, they tend to lack the specificity and resilience required in order to effectively control new types of online content. In addition, the ruling emphasized the urgent necessity for enhanced training of police officers in cybercrime investigation, citing that without technical awareness and knowledge, justice in such highly digitalized cases may be delayed or denied. The case emphasized the urgent need for tighter content moderation policies, legal reform, and infrastructure development to address the changing nature of cybercrimes, especially those that overlap with personal privacy and mental health.[16]

4. Social Concerns in respect of Cyber Bullying

4.1. Psychological Effects:

Cyberstalking and cyberbullying victims usually suffer from considerable psychological distress. These effects are:

Anxiety and Depression: Harassment fear and the emotional stress of cyberbullying can contribute to chronic stress, anxiety, and depression.

Isolation and Social Withdrawal: Teenagers victimized by cyberbullying can start withdrawing from social contact, both online and offline, to escape further victimization.[17]

Low Self-Esteem: Cyberbullying often attacks one's self-worth, resulting in feelings of inadequacy and negative body image.

Suicidal Thoughts: In extreme instances, severe online harassment may even result in suicidal thoughts, with the victim feeling trapped and hopeless.

Decline in Studies: The pressure created by cybercrimes may hinder an adolescent's concentration towards studies, resulting in declining academic performance.[18]

4.2. Cultural Factors

Family Expectations: The focus on family reputation in Indian culture makes the shame resulting from cyberbullying and cyberstalking even more significant for victims and their families.

Stigma Surrounding Mental Health: Social stigma regarding mental health in India discourages many teenagers from seeking assistance or openly talking about their issues.

Lack of Awareness: Low awareness regarding cyberbullying and cyberstalking among parents and teachers can slow down timely support and intervention for victims.[19]

4.3. Bullying in Indian Educational Institutions

India does not yet have a dedicated law specifically aimed at addressing bullying in schools, but the problem is as rampant and pervasive as ever. The lack of an enveloping law has yet to deter government agencies from taking action against such behaviour. The Ministry of Education (previously Ministry of Human Resource Development) has instructed schools to form anti-ragging or disciplinary committees to handle and contain acts of bullying. In the worst cases, punishment in the form of suspension or expulsion (rustication) may be used against perpetrators.

At the university and college level, the University Grants Commission (UGC) has enforced more stringent regulations. All UGC-recognized institutions must form anti-ragging committees and implement the "UGC Regulations on Curbing the Menace of Ragging in Higher Educational Institutions, 2009" strictly. Failure to follow these guidelines may result in the withdrawal of UGC recognition from the institution in question.

Legally, students of colleges who are convicted of cyberbullying may be subjected to criminal trials according to the Bharatiya Nagarik Suraksha Sanhita, 2023. There is, however, a significant loophole in legal protection for students of schools who are being bullied or cyberbullied. The Bharatiya Nyaya Sanhita, 2023 (BNS) and BNSS fail to offer such victims in schools any specific remedies. One reason for this is that school-aged children are treated as juveniles under the Juvenile Justice Act, where rehabilitation is stressed rather than punishment. The legal system thus does not impose similar stringent provisions on them as it would on adults. To navigate the intricacies of bullying and its legal aspects—particularly with reference to cybercrime—it is best to consult experts who specialize in cyber law and juvenile justice.[20]

5. Reforms and Comparative Analysis on Cyberbullying and Cyberstalking

5.1. India's Legal Reforms:

IT Act Amendments have widened definitions and punishments for online harassment, including the recognition of revenge porn.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate due diligence by social media intermediaries, including the appointment of grievance redressal officers, time-bound removal of unlawful content, and traceability of originators of messages. These provisions aim to address anonymity and improve accountability in cases of cyberbullying and cyberstalking.[21]

The National Cybercrime Reporting Portal facilitates easier and centralized reporting of online crimes, facilitating law enforcement response.

5.2. Global Comparisons:

United States: State laws against cyberbullying are present, backed by federal school resources.

United Kingdom: The Online Safety Bill legally obliges technology companies to address harms on the internet.

Canada: Provincial and federal legislation deals with cyberbullying; public campaigns such as Bullying.org provide support for victims.

Australia: The eSafety Commissioner deals with online abuse; anti-cyberbullying programs are operated in schools, backed by national resources.

5.3. Comparative Insights:

Whereas India has progressed in taking proactive legislative measures, other nations such as the US, UK, Canada, and Australia have better-developed legal frameworks, mostly with embedded education and victim services.

6. Mechanisms for Reporting Cybercrimes in India

Due to the rising prevalence of cyberstalking, cyberbullying, and other cybercrimes, it is important that victims know the appropriate avenues for seeking legal assistance and reporting cybercrimes. India has put in place a number of mechanisms to enable timely action and victim access to justice and support services:

Filing an FIR at the Local Police Station

Victims may go to their local police station to file a First Information Report (FIR). According to a Supreme Court judgment, no police officer can refuse to file an FIR for a cognizable cybercrime. If the local police prove to be unwilling, victims may visit the Cyber Crime Cells, which are present in most cities and operate as special units to deal with technology-based crimes.

Online Complaint through the National Cyber Crime Reporting Portal: The Ministry of Home Affairs has set up a centralized portal – *https://cybercrime.gov.in* – through which victims can register their complaints online. This interface enables one to report particular types of cybercrimes, such as cyberbullying, stalking, child pornography, financial fraud, and so on. The portal is especially helpful for victims who feel apprehensive about going in person to the law enforcement authorities and offers anonymity for particular categories such as child abuse or sexual exploitation.

Cybercrime Helpline Number – 1930:

The Government of India has marked 1930 as the cybercrime helpline number. It mainly serves the victims of digital financial scams like unauthorized money transactions or phishing frauds. Victims are assisted by trained operators in taking immediate action, like stopping fraudulent transactions, and connecting them to the correct cybercrime police unit for additional action.

6.1. Promoting Digital Awareness and Empathy

Teachers at all levels—schools, colleges, and universities—are responsible for assisting teenagers in handling the digital environment responsibly. Teachers must try to develop healthy online habits and encourage ethical behaviour while interacting online. By teaching students to develop good judgment, teachers can encourage values like mutual respect, online safety, empathy, and awareness of the possible implications of irresponsible online behaviour. As pointed out by Asefeh (2007), parents and teachers must work together to increase awareness on cyberbullying and cybercrime, with a major focus on youth safety and well-being.[22]

These mechanisms will work to ensure that reporting becomes easier, more responsive, and victim-centric, and in the process, encourage a safer digital world and enhance public confidence in the cyber law enforcement mechanism. Apart from this, certain preventive strategies can be adopted.

6.2. Prevention Strategies:

Awareness & Education: Encouraging awareness about digital abuse and preventive measures via public and school education.

Robust Legal Measures: Passing concrete, enforceable laws specifically written to combat cybercrimes.

Reporting Mechanisms: Having convenient mechanisms for reporting offenses by victims.

Victim Support: Providing psychological and legal support to the victims.[23]

7. Conclusion and Recommendations

Cyberstalking and cyberbullying are some of the most alarming forms of digital abuse of the contemporary era. As internet access and social media usage continue to grow exponentially, particularly among young adults and teenagers, India is experiencing an alarming increase in technology-enabled harassment. These crimes tend to induce severe emotional and psychological trauma, which can be aggravated to depression, anxiety, and even suicide. The anonymity and accessibility of the net only encourage perpetrators further, while victims often find it difficult to access legal remedies or emotional coping. While India has taken steps in defining cyberstalking via provisions in law such as Section 78 of the BNS, cyberbullying is still undefined in law and underregulated to a large extent, leaving an enormous protection deficit and gap in enforcement. In addition, mechanisms available—legal and administrative—do not have the consistency, speed, and victim-focused strategy required to adequately counter the ever-changing dynamics of online attacks.

Against these shortfalls, the following suggestions are imperative:

Enact Specific Cyberbullying Legislation:

A specific law defining cyberbullying, its forms, and proportionate penalties is necessary to ensure uniform enforcement and delivery of justice.

Incorporate Cyber Hygiene Education in Schools:

Educating children about good online conduct, online safety, and the psychological effects of cybercrimes at a young age can lead to safer online communities and equip young users to report abuse.

Sensitize and Train Police and Judiciary

Specialized training programs must be introduced to enable law enforcement officers and judges to deal with cybercrime cases sensitively and effectively, particularly those involving women and children.

Mandate Accountability of Digital Platforms:

Social media platforms and digital service providers need to be held accountable for not moderating objectionable content. A regulatory environment imposing timely takedowns and user safety policies is required.

Improve Forensic and Cyber Intelligence Capabilities:

Improving the technical infrastructure for cyber forensics, traceability of data, and online surveillance is key to identifying and prosecuting criminals, especially the anonymous ones.

In conclusion, India should adopt a multi-faceted approach—legal, educational, and technological—to effectively address cyberstalking and cyberbullying. The need to renovate current cyber laws, improve institutional capacity, and underscore victim welfare is no longer discretionary but necessary to protect the mental health and dignity of citizens in the digital world.

REFERENCES

[1] Varshney, R. 2024.Victims of Cyberbullying and Cyberstalking: An Exploratory Study of Harassment Perpetrated via the Internet. Library Progress - Library Science, Information Technology & Computer, 44(3).

[2] Prateeksha, K.N. 2022.Regulation of Cyberbullying in India: A Study. Indian Journal of Law and Legal Research, 4(1).

[3] Reyns, B.W., Henson, B. and Fisher, B.S. 2012.Cyberstalking Victimization: An Examination of Routine Activity Theory and Social Learning Theory. Journal of Investigative Psychology and Offender Profiling, 9: 277.

[4] Kowalski, R.M., Giumetti, G.W., Schroeder, A.N. and Lattanner, M.R. 2014.Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth. Psychological Bulletin, 140: 1073.

[5] De Pedro, K.T. et al. 2014.School Climate Perceptions Among Students in Military-Connected Schools: A Comparison of Military and Nonmilitary Students in the Same Schools. Military Behavioral Health, 2: 3.

[6] Drouin, M., Vogel, K.N., Surbey, A., Stills, J.R. and Patel, D. 2017.Let's Talk About Sexting, Baby: Computer-Mediated Sexual Behaviors Among Young Adults. Computers in Human Behavior, 77: 372.

[7] Buckels, E.E., Trapnell, P.D. and Paulhus, D.L. 2014.Trolls Just Want to Have Fun. Personality and Individual Differences, 67: 97.

[8] Nixon, C.L. and Ronson, J. 2018.So You've Been Publicly Shamed: A Psychological Perspective. Journal of Applied Social Psychology, 48: 629.

[9] Charan, J.L. Cyber Stalkers and Cyberbullies: Protecting Women in the Digital Age. Cyber Crime, : 119.

[10] Digital Personal Data Protection Act. 2023.India Code, No. 22 of 2023.

[11] Rachna and Varshney, R. 2024.Cyberbullying and Cyberstalking Laws in India: Legal Barriers to Prevent Cybercrime. Cahiers Magellanes-NS, 6(2): 2182.

[12] Chhavi. 2023.Online Laws Against Cyberbullying and Online Harassment in India. Jus Corpus Law Journal, 4: 771.

[13] Prashasti, G.V.L. 2025.Vagueness, Overbroad Powers and the Chilling Effect: Section 66A vs Article 19(1)(a) in Shreya Singhal v. Union of India. International Journal of Law and Legal Research.

[14] Shekhawat, H. 2022.Cyber Crimes Against Women. International Journal of Law Management and Humanities, 5: 1673.

[15] Bhavitha, L. 2023.Cyber Crime: Is It Any Worse Than a Crime? Indian Journal of Law and Legal Research, 5(1).

[16] Maheshwari, R. 2021.Changing Paradigms of Victimization in Cybercrimes: An Analysis. International Journal of Law Management and Humanities, 4: 2871.

[17] Roy, S. and Samanta, A. 2020.An Analysis of Online Harassment and Cyberbullying in India: Perceptions and Experiences. Computers in Human Behavior, 105: 106216.

[18] Constitution of India. Article 21.

[19] Information Technology Act. 2000.India Code, No. 21 of 2000.

[20] Khudhair, N.S. 2021.Cyberbullying – A Critical Analysis of Laws, Criminal Responsibility and Jurisdiction. Journal of Contemporary Issues in Business and Government, 27: 2644.

[21] Kumar, A. 2022.Intermediary Liability and Accountability under the Information Technology Rules, 2021: A Critical Analysis. Journal of Cyber Law and Policy, 7(2): 45–60.

[22] Nosrat, A. 2007.To Investigate the Relationships Between Awareness and Use of Digital Resources Among Students. Isfahan University of Medical Sciences.

[23] Rachna and Varshney, R. 2024.Cyberbullying and Cyberstalking Laws in India: Legal Barriers to Prevent Cybercrime. Cahiers Magellanes-NS, 6: 2182.