VOLUME 6 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CYBERSTALKING AND ONLINE HARASSMENT: EVALUATING THE EFFECTIVENESS OF THE INDIAN LEGAL FRAMEWORK

- Priyanshi Modi* & Dr. Nidhi Sharma*

Abstract

The rapid expansion of digital communication technologies has significantly transformed social interaction in India while simultaneously creating new avenues for cybercrime. Among these emerging threats, cyberstalking and online harassment have become increasingly prevalent forms of digital abuse, particularly affecting women and vulnerable groups. Despite the existence of legislative provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and related regulatory frameworks, the effectiveness of these laws in addressing cyberstalking remains questionable. This research paper examines the adequacy of India's current legal framework in combating cyberstalking and online harassment. Using a doctrinal research methodology, the study analyses statutory provisions, judicial decisions, and scholarly literature to identify legal gaps and enforcement challenges. The paper further evaluates landmark judicial precedents such as Shreya Singhal v. Union of India and explores issues including jurisdictional complexity, technological barriers in investigation, and underreporting of cyber harassment cases. The research concludes that although India has made legislative progress in regulating cybercrime, the current framework remains insufficient due to vague statutory definitions, lack of victim-centric protections, and limited technological capacity within law enforcement agencies. The paper recommends comprehensive legal reforms, clearer statutory definitions, enhanced platform accountability, and specialized cybercrime enforcement mechanisms to strengthen protection against cyberstalking and online harassment in India.

Keywords: *Cyberstalking, Online Harassment, Cybercrime Law, Information Technology Act, Bharatiya Nyaya Sanhita, Digital Rights*

*LLM (Criminal Justice System)Centre for Legal Studies, Gitarattan International Business School, Delhi
*Associate Professor Centre for Legal Studies, Gitarattan International Business School, Delhi

INTRODUCTION

The rapid development of digital technologies has fundamentally transformed the nature of communication, social interaction, and access to information in the modern world. Over the past two decades, the internet has evolved from a limited technological infrastructure into an essential component of everyday life. Individuals now rely on digital platforms for communication, professional engagement, education, commerce, and participation in public discourse. In India, the digital revolution has been particularly significant due to the widespread adoption of smartphones, affordable internet services, and government initiatives promoting digital inclusion. As a result, India currently possesses one of the largest populations of internet users globally, with millions of individuals engaging in online activities through social media platforms, messaging applications, and other digital services.[1]While the growth of digital communication technologies has created numerous opportunities for economic development and social connectivity, it has also introduced new forms of criminal behaviour that exploit the vulnerabilities of online environments. Cybercrime has emerged as a major challenge for legal systems worldwide, requiring governments to develop regulatory frameworks capable of addressing offenses that occur within digital spaces. Among the various forms of cybercrime, cyberstalking and online harassment have become particularly significant due to their widespread impact on individual safety, privacy, and psychological well-being. Cyberstalking can be broadly defined as the use of electronic communication technologies to repeatedly harass, threaten, monitor, or intimidate an individual through digital platforms.[2] Unlike traditional stalking, which typically involves physical surveillance or direct contact, cyberstalking allows perpetrators to engage in abusive behaviour through electronic communication channels such as social media platforms, email services, and messaging applications. The anonymity and accessibility of the internet enable offenders to conceal their identities and operate across geographical boundaries, thereby complicating efforts to identify and prosecute perpetrators.Online harassment represents a broader category of digital abuse that includes a wide range of behaviours such as abusive messaging, impersonation, dissemination of private information, image-based sexual abuse, and coordinated trolling campaigns. These forms of harassment frequently occur on social media platforms, where individuals may be targeted by large groups of users engaging in coordinated harassment. Research indicates that victims of

[1]Internet & Mobile Ass'n of India, Digital in India Report 2023
[2]Michael Pittaro, Cyberstalking: An Analysis of Online Harassment and Intimidation, 1 Int'l J. Cyber Criminology 180 (2007).

online harassment often experience severe psychological distress, including anxiety, depression, and feelings of social isolation.[3] The persistent nature of digital harassment further exacerbates these effects, as victims may find it difficult to escape abusive behavior in online spaces that are deeply integrated into their daily lives. The growing prevalence of cyberstalking and online harassment has raised serious concerns regarding the adequacy of existing legal frameworks to address these forms of digital abuse. Traditional criminal laws were primarily designed to regulate conduct occurring within physical environments and often struggle to adapt to the unique characteristics of cyberspace. Digital platforms allow individuals to communicate instantaneously across national borders, creating jurisdictional complexities that can hinder effective law enforcement. Furthermore, the anonymity provided by digital communication technologies enables perpetrators to evade identification, making it difficult for authorities to gather sufficient evidence to support criminal prosecutions.

In India, the legal framework governing cybercrime has evolved gradually in response to the increasing use of digital technologies. The Information Technology Act, 2000 represents the primary legislation regulating cyber activities and addressing various forms of digital offenses. The Act introduced several provisions aimed at criminalizing hacking, identity theft, and the transmission of obscene content through electronic means.[4] Over time, additional regulatory mechanisms have been introduced to address emerging digital challenges, including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose due diligence obligations on online intermediaries such as social media platforms.

More recently, the introduction of the Bharatiya Nyaya Sanhita, 2023 has replaced the Indian Penal Code and incorporated provisions addressing offenses such as stalking and voyeurism.[5] Although these provisions may be applied to cases involving cyberstalking, they were primarily designed to address physical forms of harassment and may not adequately capture the complexities of digital abuse. In addition, the enactment of the Digital Personal Data Protection Act, 2023 represents an important step toward strengthening data privacy protections in India, which may indirectly contribute to the prevention of cyber harassment by regulating the misuse of personal information.

[3]Debarati Halder & K. Jaishankar, Cyber Crimes Against Women in India (2016).
[4]Information Technology Act, No. 21 of 2000, India Code (2000).
[5]Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).

Judicial interpretation has played an important role in shaping the legal framework governing online speech and cybercrime in India. The landmark decision of the Supreme Court in *Shreya Singhal v. Union of India* represents a pivotal moment in the development of Indian cyber law. In this case, the Court declared Section 66A of the Information Technology Act unconstitutional on the grounds that it violated the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution.[6] While the decision strengthened constitutional protections for online speech, it also created a regulatory gap in addressing certain forms of online harassment and abusive communication. In light of these developments, it is essential to critically examine whether the existing legal framework in India is capable of effectively addressing cyberstalking and online harassment. The rapid evolution of digital technologies requires legal systems to continuously adapt in order to protect individuals from emerging forms of abuse while preserving fundamental rights such as freedom of expression and privacy.

This research paper seeks to evaluate the effectiveness of India's current legal framework in regulating cyberstalking and online harassment. By analyzing statutory provisions, judicial interpretations, and enforcement challenges, the study aims to identify gaps within existing laws and propose reforms that could strengthen legal protections for victims of digital harassment. Through a comprehensive examination of the intersection between cybercrime regulation and digital rights, the paper contributes to the broader discourse on the role of law in governing online behaviour within an increasingly interconnected digital society.

LEGAL FRAMEWORK GOVERNING CYBERSTALKING IN INDIA

The rapid expansion of digital communication technologies has significantly increased the prevalence of cybercrime, including cyberstalking and online harassment. In response to these challenges, India has developed a legal framework comprising several statutes and regulatory instruments aimed at governing digital conduct and addressing cyber offenses. Although India does not currently have a single comprehensive statute specifically dedicated to cyberstalking, various provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Digital Personal Data Protection Act, 2023 collectively attempt to regulate forms of online harassment and digital abuse. These laws address different aspects of cybercrime, including privacy violations, digital content

[6]Shreya Singhal v. Union of India, (2015) 5 SCC 1.

regulation, platform accountability, and data protection. However, despite these legislative measures, several legal gaps and enforcement challenges remain in effectively combating cyberstalking within India's digital ecosystem.

Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) represents the cornerstone of India's cybercrime legislation and was enacted to provide legal recognition for electronic transactions and to address emerging cyber offenses associated with the use of digital technologies.[7] The Act introduced a range of provisions aimed at regulating digital communication, protecting electronic data, and criminalizing unauthorized access to computer systems. Over time, amendments to the IT Act have expanded its scope to include various forms of cybercrime, including identity theft, privacy violations, and the dissemination of obscene digital content. Several provisions of the IT Act are particularly relevant in addressing conduct associated with cyberstalking and online harassment. Section 66E criminalizes the violation of privacy through the capture, publication, or transmission of images of a private area of an individual without their consent.[8] This provision is significant in cases involving non-consensual image sharing or voyeuristic digital conduct, which often forms part of online harassment. The section prescribes imprisonment of up to three years or a fine of up to two lakh rupees, or both, for individuals who engage in such activities.

Section 67 of the IT Act further criminalizes the publication or transmission of obscene material in electronic form.[9] This provision is frequently invoked in cases involving the circulation of sexually explicit content, revenge pornography, or other forms of digital harassment that involve sexually explicit material. Section 67A provides additional penalties for the transmission of material containing sexually explicit acts, while Section 67B addresses the dissemination of child sexual abuse material. Another relevant provision is Section 69, which empowers the government to intercept, monitor, or decrypt electronic communications in the interest of national security, public order, or the prevention of crime.[10] Although this provision is primarily designed for national security purposes, it can also play a role in cybercrime investigations by enabling authorities to trace digital communications used in harassment or stalking cases.

[7] Information Technology Act, No. 21 of 2000, India Code (2000)
[8] Information Technology Act § 66E (2000).
[9] Information Technology Act § 67 (2000).
[10] Information Technology Act § 69 (2000).

One of the most controversial provisions of the IT Act was Section 66A, which criminalized the sending of "offensive" messages through communication services.[11] This provision was widely criticized for its vague language and broad scope, which allowed authorities to prosecute individuals for online speech that was deemed offensive or inconvenient. In the landmark judgment *Shreya Singhal v. Union of India*, the Supreme Court of India struck down Section 66A as unconstitutional on the grounds that it violated the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution.[12]

The Court held that the provision was excessively vague and created a chilling effect on free speech by allowing arbitrary enforcement. While the judgment was widely welcomed as a victory for digital free expression, it also removed a statutory provision that had previously been used to prosecute certain forms of online harassment. As a result, law enforcement agencies have since relied on alternative provisions under the IT Act and other criminal laws to address cyber harassment cases. Despite its significance, the IT Act has often been criticized for failing to adequately address the complexities of cyberstalking. The Act primarily focuses on technical offenses such as hacking and data theft, rather than providing a comprehensive legal framework specifically designed to regulate online harassment and digital stalking behaviour.

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita (BNS), enacted in 2023 to replace the Indian Penal Code of 1860, introduced updated provisions aimed at modernizing India's criminal law framework.[13] Among its provisions are sections addressing stalking, voyeurism, and harassment, which may be applied to cyberstalking cases. Section 78 of the BNS criminalizes stalking behaviour, including repeated attempts to contact a woman or monitor her activities despite clear indications of disinterest.[14] The provision recognizes that stalking may occur through electronic communication and includes acts such as monitoring an individual's use of the internet, email, or other electronic communication platforms. The inclusion of digital monitoring within the definition of stalking represents an important step toward recognizing cyberstalking as a form of criminal conduct. However, despite this recognition, the provision was primarily drafted with traditional stalking in mind and therefore does not fully capture

[11] Information Technology Act § 66A (2000).
[12] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[13] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).
[14] Bharatiya Nyaya Sanhita § 78 (2023).

the complexity of modern cyber harassment. Digital stalking can involve a wide range of behaviours, including online impersonation, doxxing, coordinated trolling campaigns, and the creation of fake social media accounts for harassment purposes. These behaviours may not always fall neatly within the statutory definition of stalking.

Another relevant provision is Section 79 of the BNS, which criminalizes acts intended to insult the modesty of a woman.[15] This provision may be invoked in cases involving sexually explicit harassment or abusive communication directed toward women on digital platforms. While the Bharatiya Nyaya Sanhita represents a significant reform of India's criminal law framework, legal scholars have noted that the statute still lacks comprehensive provisions specifically designed to address cyber harassment and online abuse. The absence of detailed definitions and specialized investigative mechanisms continues to create challenges in prosecuting cyberstalking cases.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 represent a regulatory framework aimed at enhancing the accountability of digital intermediaries such as social media platforms, messaging services, and online marketplaces.[16] These rules were introduced under Section 79 of the Information Technology Act and impose due diligence obligations on intermediaries to prevent the misuse of their platforms for unlawful activities.

One of the key features of the 2021 Rules is the requirement that intermediaries establish effective grievance redressal mechanisms to address user complaints. Social media platforms must appoint grievance officers responsible for receiving and resolving complaints related to unlawful content, including harassment and abusive communication.[17] Platforms are also required to acknowledge complaints within twenty-four hours and resolve them within fifteen days. The Rules further require intermediaries to remove or disable access to unlawful content within specific timeframes upon receiving a valid complaint or government order. This provision is particularly relevant in cases involving cyber harassment, where harmful content such as defamatory posts, non-consensual intimate images, or abusive messages may

[15] Bharatiya Nyaya Sanhita § 79 (2023).
[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[17] Id. r. 3

need to be removed quickly to prevent further harm to victims. Additionally, significant social media intermediaries are required to appoint compliance officers and nodal contact persons responsible for ensuring adherence to the regulatory framework. These requirements aim to increase corporate accountability for addressing harmful content on digital platforms.

However, the Rules have also generated considerable debate regarding their implications for privacy and freedom of expression. Critics argue that certain provisions, particularly those requiring traceability of messages on encrypted platforms, may undermine user privacy and enable government surveillance. Despite these concerns, the Rules represent an important regulatory mechanism for addressing online harassment by placing greater responsibility on digital platforms to moderate harmful content.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive legislation regulating the processing and protection of personal data.[18] The Act establishes a framework governing how organizations collect, store, process, and share personal data, while also providing individuals with rights over their personal information. Although the DPDP Act is not specifically designed to address cyberstalking or online harassment, it plays an important role in strengthening privacy protections within India's digital ecosystem. Many forms of cyber harassment involve the misuse of personal information, such as the unauthorized sharing of personal data, images, or contact details. By establishing stricter data protection requirements, the DPDP Act may help reduce opportunities for such misuse.

The Act introduces the concept of "data fiduciaries," which refers to entities responsible for processing personal data. Data fiduciaries are required to obtain consent from individuals before processing their personal data and must implement reasonable security safeguards to prevent data breaches.[19] In the event of a data breach, organizations must notify the Data Protection Board of India and affected individuals.

The DPDP Act also grants individuals several rights, including the right to access information about how their data is processed and the right to request correction or erasure of inaccurate

[18] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[19] Id. § 8

data. These rights may assist victims of cyber harassment in seeking the removal of harmful or misleading information from digital platforms. However, while the Act strengthens privacy protections, it does not directly criminalize cyber harassment or provide specific remedies for victims of online abuse. As a result, its role in addressing cyberstalking remains largely indirect, functioning primarily as a mechanism for protecting personal data rather than regulating digital conduct.

JUDICIAL INTERPRETATION AND CASE LAW ANALYSIS

Judicial interpretation has played a crucial role in shaping the legal landscape governing cyberstalking and online harassment in India. In the absence of a comprehensive statutory framework specifically addressing cyber harassment, courts have frequently relied on constitutional principles, existing cyber laws, and traditional criminal law provisions to resolve disputes involving digital misconduct. Through various landmark decisions, the judiciary has attempted to balance fundamental rights such as freedom of speech and privacy with the need to protect individuals from online abuse and harassment.

Shreya Singhal v. Union of India: Constitutional Limits on Regulation of Online Speech

One of the most significant judicial decisions shaping cyber law in India is the Supreme Court's judgment in *Shreya Singhal v. Union of India*.[20] The case challenged the constitutional validity of Section 66A of the Information Technology Act, 2000, which criminalized the sending of offensive messages through electronic communication services.

Section 66A penalized the sending of messages that were "grossly offensive" or caused "annoyance" or "inconvenience." Petitioners argued that the provision was vague and overly broad, enabling arbitrary arrests for legitimate online expression. The Supreme Court examined whether the provision violated the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution.

The Court held that Section 66A was unconstitutional because its language was vague and lacked clear definitions. The terms used in the provision were subjective and could easily be misinterpreted by law enforcement authorities. The Court further observed that the provision

[20] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

created a chilling effect on free speech by discouraging individuals from expressing opinions online for fear of prosecution.

As a result, the Supreme Court struck down Section 66A in its entirety. While the judgment significantly strengthened constitutional protections for digital expression, it also created a regulatory gap in addressing certain forms of online harassment that had previously been prosecuted under the provision. Consequently, authorities now rely on alternative statutory provisions under the Information Technology Act and criminal law statutes to address cyber harassment.

Ritu Kohli v. Manish Kathuria: One of the First Cyberstalking Cases in India

The case of *Ritu Kohli v. Manish Kathuria* is widely regarded as one of the earliest reported cases of cyberstalking in India.[21] The accused created a fake online profile in the name of the victim on internet chat forums and posted her personal contact details while falsely claiming that she was offering sexual services.

As a consequence, the victim began receiving numerous obscene phone calls from strangers who had seen the online postings. At the time of the incident, India did not have specific legislation addressing cyberstalking or online impersonation. Therefore, the accused was prosecuted under Section 509 of the Indian Penal Code, which criminalized acts intended to insult the modesty of a woman.

This case highlighted the limitations of traditional criminal law in addressing cybercrimes that arise in digital environments. It demonstrated that existing provisions were not adequately designed to deal with online impersonation, identity theft, and cyber harassment. The case subsequently contributed to the growing recognition of cyberstalking as a distinct form of cybercrime requiring specialized legal regulation.

Avinash Bajaj v. State (NCT of Delhi): Intermediary Liability for Online Content

The issue of intermediary liability in cybercrime cases was addressed by the Delhi High Court in *Avinash Bajaj v. State (NCT of Delhi)*.[22] The case involved the sale of an obscene video clip through an online marketplace platform. The prosecution sought to hold the

[21] State v. Manish Kathuria, C.C. No. 14616/2014 (Delhi Dist. Ct.)
[22] Avinash Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427 (Del. HC).

managing director of the company personally liable for hosting illegal content on the website. The central issue before the court was whether an intermediary could be held criminally liable for user-generated content uploaded by third parties.

The Delhi High Court held that intermediaries should not automatically be held liable for all content hosted on their platforms, provided they exercise due diligence and act promptly to remove unlawful material when notified. The court emphasized that the liability of intermediaries must be assessed in light of the due diligence obligations imposed by the Information Technology Act. This decision significantly influenced the development of intermediary liability principles in India and later informed the regulatory framework established under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The case illustrates the judiciary's effort to balance the responsibilities of digital platforms with the need to prevent the misuse of online services for illegal activities.

Nipun Saxena v. Union of India: Protection of Victim Identity and Digital Privacy

Another important judicial decision relevant to cyber harassment and digital privacy is *Nipun Saxena v. Union of India*.[23] Although the case primarily concerned the protection of rape victims' identities, the Supreme Court's observations have broader implications for online harassment and digital privacy.

The Court emphasized that the disclosure of victims' identities through digital platforms, social media, or other online forums can cause severe psychological harm and further victimization. It directed that the identities of victims of sexual offenses must not be disclosed in any form, including through electronic media. The judgment reinforced the importance of protecting personal data and privacy in the digital age. It also highlighted the need for stricter regulation of the dissemination of sensitive personal information on digital platforms, which is particularly relevant in cases involving cyberstalking and online harassment.

Judicial Trends and the Need for Legislative Reform

[23] Nipun Saxena v. Union of India, (2019) 2 S.C.C. 703 (India).

The above cases illustrate the evolving role of the judiciary in addressing cyberstalking and online harassment within the constraints of existing legal frameworks. Courts have attempted to interpret traditional legal provisions in ways that accommodate emerging forms of digital misconduct. However, reliance on judicial interpretation alone is insufficient to effectively regulate cyber harassment.

These cases highlight the urgent need for comprehensive legislation specifically addressing cyberstalking and online harassment. Clear statutory definitions, specialized investigative mechanisms, and stronger regulatory obligations for digital platforms are necessary to ensure effective protection for victims of cyber abuse.

RECOMMENDATIONS FOR LEGAL REFORM

The increasing prevalence of cyberstalking and online harassment in India highlights significant gaps within the current legal framework governing cybercrime. Although statutes such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provide certain mechanisms to address online abuse, these provisions remain fragmented and insufficient to effectively combat the evolving nature of cyber harassment.

One of the most important reforms required is the enactment of a comprehensive legal framework specifically addressing cyberstalking and online harassment. Currently, cyberstalking cases are prosecuted under a combination of provisions relating to privacy violations, obscenity, and stalking under different statutes. This fragmented approach often creates interpretational difficulties and limits the ability of law enforcement authorities to prosecute offenders effectively. A dedicated cyberstalking law should clearly define various forms of digital harassment, including impersonation, doxxing, image-based abuse, and persistent online surveillance.

Another essential reform involves the development of victim-centric legal remedies that enable faster and more effective responses to cyber harassment. Victims of online abuse often experience severe psychological harm due to the rapid dissemination of harmful content through digital platforms. Therefore, the legal framework should introduce mechanisms such as digital protection orders or online restraining orders, which would allow courts to immediately restrict offenders from contacting victims or publishing harmful material online.

Strengthening the investigative capacity of law enforcement agencies is also critical for improving the enforcement of cybercrime laws. Many cyberstalking cases remain unresolved due to the lack of specialized cybercrime units and digital forensic expertise within police departments. The government should invest in training programs that equip law enforcement personnel with the technical knowledge required to investigate cyber offenses. Establishing dedicated cybercrime investigation units in major cities and strengthening collaboration between law enforcement agencies and digital platforms would significantly improve the detection and prosecution of cyber offenders.

Another important reform involves enhancing the accountability of digital intermediaries and social media platforms. Digital platforms play a central role in facilitating communication and content sharing, and they must therefore take greater responsibility in preventing the misuse of their services for harassment and abuse. The Information Technology Rules, 2021 already impose certain due diligence obligations on intermediaries, including the requirement to establish grievance redressal mechanisms. However, these provisions should be further strengthened to ensure that platforms respond promptly to complaints involving cyberstalking and harassment.

Finally, addressing cyberstalking requires greater international cooperation in cybercrime enforcement. The borderless nature of the internet allows perpetrators to operate across multiple jurisdictions, making it difficult for national authorities to investigate and prosecute offenders. India should therefore strengthen its participation in international cybercrime cooperation frameworks and develop bilateral agreements with other countries to facilitate information sharing and cross-border investigations.

1. CONCLUSION

Cyberstalking and online harassment have emerged as pressing challenges within the rapidly expanding digital environment. As digital technologies continue to transform communication, social interaction, and economic activity, they have simultaneously created new avenues for misuse and abuse. The anonymity, accessibility, and borderless nature of the internet enable offenders to target individuals with relative ease, often making it difficult for victims to identify perpetrators or seek timely legal remedies. In India, the increasing use of social media platforms and digital communication tools has further intensified the prevalence of

cyber harassment, particularly affecting women, young individuals, and other vulnerable groups.

Although India has introduced several legislative measures to address cybercrime, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Digital Personal Data Protection Act, 2023, these laws collectively remain insufficient to address the full complexity of cyberstalking and online harassment. The current legal framework largely relies on provisions that were either designed to regulate technical cyber offenses or traditional forms of harassment, rather than the multifaceted nature of digital abuse.

Furthermore, the absence of clear statutory definitions for cyberstalking and related forms of digital harassment significantly weakens the effectiveness of legal enforcement. Technological limitations within investigative agencies, jurisdictional challenges arising from cross-border cyber activities, and the persistent problem of underreporting further complicate efforts to address cyber harassment effectively. Judicial interventions have attempted to bridge some of these gaps through interpretational developments, yet reliance on judicial interpretation alone cannot substitute for comprehensive legislative reform.

Addressing the growing threat of cyberstalking requires a multi-dimensional approach that combines legal reform, institutional capacity building, and stronger accountability mechanisms for digital platforms. The development of specialized cybercrime units, enhanced digital forensic capabilities, and improved cooperation between law enforcement agencies and technology companies are essential for strengthening enforcement mechanisms. Additionally, victim-centered policies, including rapid grievance redressal systems and stronger privacy protections, must be integrated into the legal framework to ensure effective protection for individuals targeted by online abuse.

In conclusion, safeguarding individuals from cyberstalking and online harassment is essential for maintaining trust and security in digital spaces. By adopting comprehensive legal reforms and strengthening institutional mechanisms, India can develop a more effective regulatory framework capable of addressing the evolving challenges of cybercrime while simultaneously protecting fundamental rights in the digital age.

BIBLIOGRAPHY

A. Amit Kumar , Dr. Dalip Kumar, "Crimes of Stalking and Harassment Against Women in Cyberspace", International Journal for Multidisciplinary Research, Volume 5, Issue 6, (2023) https://www.ijfmr.com/papers/2023/6/9006.pdf

B. Pooja, "The Growing Threat of Cyberbullying in India", IJERED, Vol. 11 Issue 4 (2023) https://www.researchgate.net/publication/372724976_The_Growing_Threat_of_Cyberbullying_in_India

C. Aadya Dipti, "Cyber Stalking and Harassment in India - A Matter of Great Concern", Indian J.L. & Legal Rsch, Vol:II, Issue: I, (2021) https://heinonline.org/HOL/LandingPage?handle=hein.journals/injlolw2&div=104&id=&page=

D. Rohini Chahal , Lovish Kumar , Shivam Jindal and Poonam Rawat, "Cyber Stalking: Technological Form of Sexual Harassment", International Journal on Emerging Technologies 10(4): 367-373(2019) https://d1wqtxts1xzle7.cloudfront.net/103596806/Cyber-Stalking-Technological-Form-of-Sexual-Harassment.pdf?1687319179=&response-content-disposition=inline%3B+filename%3DCyber_Stalking_Technological_Form_of_Sex.pdf&Expires=1731195724&Signature=EuPZdQOLFwfrdt43iMamha5RKPfwTEhOrY7hGIc2rd-1va-

E. Manpreet Kaur & Munish Saini, "Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions", Educ Inf Technol, Volume 28, pages 581–615, (2023) https://doi.org/10.1007/s10639-022-11168-4.

F. Saran Errakot&Rahoof VK, "Cyber bullying: A Need for Separate Provision in Indian Law", GLS LAW JOURNAL, Vol 5 No 1 (2023) https://doi.org/10.69974/glslawjournal.v5i1.81

G. https://law4u.in/answer/2976/What-is-the-punishment-for-cyberbullying-and-online-harassment-in-India

H. https://www.eap-india.com/online-harassment-meaning-types-impact/

I. https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

J. https://www.unicef.org/end-violence/how-to-stop-cyberbullying

K. https://kidshealth.org/en/teens/cyberbullying.html

L. https://www.equalrights.org/issue/covid-cyberbullying/

M. https://www.thecyberhelpline.com/guides/cyber-stalking

N. https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking

O. https://www.sciencedirect.com/topics/computer-science/cyberstalking

P. https://www.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking

Q. https://www.ijfmr.com/papers/2023/6/9006.pdf

R. https://www.jmc.ac.in/uploads/staticfiles/societies/Presentation%20Cyberstalking%20