LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S4(2025)

THE QUEST FOR JUSTICE: CYBERSTALKING AGAINST WOMEN IN INDIA

Sakshi Kaushik[1], Dr Shubrangna Pundir[2], Priya Sharma[3], Komal Dixit[4]

[1,3,4]Research scholar, School of Law at Galgotias University, Greater Noida, UP, India
[2]Assistant Professor, School of Law at Galgotias University, Greater Noida, UP, India

advsakshik@gmail.com[1],
Shubhrangana@galgotiasuniversity.edu.in[2],
priyasharma.sharma144@gmail.com[3],
dixit.komal.lko@gmail.com[4]

Abstract
Cyberstalking has emerged as a ubiquitous and growing issue in India, disproportionately affecting women and revealing gaps in the country's digital legal framework. As technology and social media continue to expand, cyberstalking has evolved into a more complex form of harassment, exacerbating gender disparities. This paper explores the prevalence and impact of cyberstalking in India, focusing on the effectiveness of the Information Technology Act (2000) and the Bhartiya Nyaya Sanhita (2023) in addressing this crime. The study highlights the inadequacies of existing laws, particularly their failure to address modern cybercrimes such as non-consensual dissemination of personal information, online harassment, and cyberstalking. High-profile case studies, including those of Ritu Kohli and Sharmistha Mukherjee, illustrate how perpetrators exploit digital anonymity to harass women without immediate legal repercussions. These cases reveal the shortcomings of current legal instruments, such as the lack of clear definitions for cyberstalking and the challenges of handling cross-jurisdictional crimes.
The research also examines law enforcement's challenges, including the lack of technical expertise to trace anonymous cyberstalkers. The paper advocates urgent legislative reforms to combat cyberstalking, including clearer legal definitions, rigorous penalties, and updated procedural guidelines. Ultimately, the paper emphasizes the need for a multi-stakeholder approach, involving law enforcement, policymakers, digital platforms, and civil society, to create a secure digital environment for women. It calls for a coordinated strategy combining legal reform and societal education to reduce cyberstalking and foster a safer and more equitable digital ecosystem for women in India.

Keywords: Cyberstalking, Women's Digital Safety, The Bhartiya Nayaya Sanhita, 2023, Information Technology Act, 2000, Cybersecurity Measures.

1. Introduction:

- Online activities may compromise personal safety and are just as susceptible to criminality as regular, daily crimes[1] (Jain, 2022). The internet and digital technology' explosive growth have altered how individuals interact, communicate, and engage with the outside world. However, cybercrime has been made possible by the digital revolution and disproportionately impacts women and other vulnerable populations[2].

According to the Seventh Schedule of the Indian Constitution, cybercrimes are state matters.[3]Cyberstalking has emerged as a significant concern in India, posing severe challenges for individuals, especially women. Cyber stalking has broken the right to privacy, which has been safeguarded under Article 21 of the Indian Constitution[4]. This was postulated in the case of *Justice K.S. Puttaswamy & Others v. Union of India & Others*[5]. The main

[1] Zero To Mastery In Information Security And Cyber Laws, by Dr. R.K. Jain, First Edition:2022
[2]https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty#:~:text=Vulnerable%20populations%E2%80%93such%20as%20women,of%20authorship%20and%20intellectual%20property .
[3] https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/LS10122024/2305.pdf
[4] https://legislative.gov.in/constitution-of-india/ , The Constitution of India
[5] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018

purpose is to instill fear in people, but social isolation is a secondary effect.[6] According to Article 51-A of the Constitution, every citizen has a fundamental obligation to preserve women's dignity, which must always be upheld.[7]

Cyberstalking involves persistent digital surveillance and intimidation, creating psychological, social, and legal challenges for victims (Rachna & Varshney, R.,2024).[8]A cybercriminal who regularly threatens someone online is engaging in cyberstalking. Email, social media, and other internet platforms are frequently used to commit this crime. When the perpetrator harasses the victim offline, cyberstalking can even happen in tandem with the other, more traditional kind of stalking. Cyberstalkers have access to a multitude of information that enables them to plan their harassment, including blogs, social media, image-sharing websites, and many other commonly utilized online sharing activities. False charges, fraud, information destruction, threats of death, and manipulation through exposure threats are some examples of such acts (Vyas Shivangi Anilkumar & Dr. Prakashkumar Thakor,2024).[9]

Hence, Cyberstalking is defined as: monitoring the victim's online activities + using a digital device or software to send harassing, threatening, abusive emails or messages, etc. + sending the said emails to the victim's inbox and/or the inboxes of the victim's friends or family members + effectively inciting feelings of fear, annoyance, irritation, and harassment in the victim.[10]

In India, where gendered inequalities are frequently enforced by social structures, the virtual world has become another area where women are at risk for many threats, including cyberstalking and online harassment[11]. Cybercrimes against women, including as online harassment, stalking, and defamation, have increased significantly in recent years, according to the National Crime Records Bureau (NCRB).[12] Cybercrimes can also lead to physical or sexual abuse.[13]Compared to 2021, there was a notable increase in cybercrimes against women in 2022. In 2022, there was an 11% rise in cybercrimes against women. The number of cases of women's sexually explicit content being transferred or published increased from 1,896 in 2021 to 2,251 cases. Additionally, 689 cybercrimes against women occurred in 2022, compared to 701 in 2021. These crimes included extortion, slander, morphing, defamation,

[6] https://indiankanoon.org/doc/127517806/ , Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018

[7] https://indiankanoon.org/doc/73866393/ ,Kalandi Charan Lenka vs State Of Odisha on 16 January, 2017, Article 51A of the Constitution Of India.

[8] Rachna, and Rahul Varshney. 2024. "CYBERBULLYING AND CYBERSTALKING: BELONGINGS AND ANTICIPATION MEASURES IN INDIA". *ShodhKosh: Journal of Visual and Performing Arts* 5 (1):1469–1476. https://doi.org/10.29121/shodhkosh.v5.i1.2024.4289.

[9] Vyas Shivangi Anilkumar, & Dr. Prakashkumar Thakor. (2024). CYBER CRIME CYBERSTALKING THROUGH THE CYBER LAW FORENSIC SCIENCE AND CRIMINAL INVESTIGATION. *International Education and Research Journal (IERJ)*, *10*(6). https://doi.org/10.21276/IERJ24924152332304

[10] Halder, Debarati and Jaishankar, K., Cyber Victimization in India: A Baseline Survey Report (2010) (December 1, 2010). Available at SSRN: https://ssrn.com/abstract=1759708 or http://dx.doi.org/10.2139/ssrn.1759708

[11]Pande R. Virtual Reality and Real Threats: Gender Violence in a Digital Age.Current Research Journal of Social Sciences and Humanities. 2024 7(2). Avialable here: https://bit.ly/4a2vb6D

[12] https://www.ncrb.gov.in/crime-in-india.html

[13] https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf

blackmail, and the creation of false profiles (Chandrashekar AR, Nandini 2023)[14]. Cyberstalking is damaging and prevalent.[15]

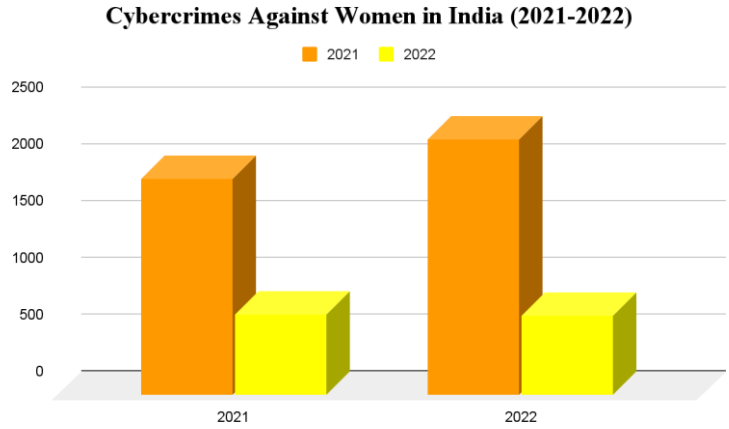

Figure 01: Cybercrimes against women in India (2021-2022)

This study utilizes literature analysis to explore cyberstalking against women in India, examining its prevalence, impact, and contributing factors to an unsafe digital environment. The first section reviews various forms of cyberstalking, including computer stalking, email stalking, webcam hijacking, and the use of stalkerware—spyware tools that enable abusers to monitor victims' activities. Data from the National Crime Records Bureau (NCRB) shows a consistent rise in cyberstalking and online harassment cases, especially against women. These crimes cause significant psychological, emotional, and social consequences, often leading victims to withdraw from cyberspace.

The second section focuses on the vulnerabilities of women in digital spaces, analyzing online abuse and the societal stigma they face. It explores how gendered violence in cyberspace exacerbates existing real-world inequalities.
The final section examines India's legal framework, assessing the effectiveness of laws and regulations in addressing cyberstalking and protecting women online. Provisions such as **Sections 354D(1), 323, 325, 321, 322, 351, 268, 354A, 509, 499 of the Indian Penal Code, 1860 (IPC)**, **Sections 354, 115(1), 115(2), 114, 115, 74, 336, 63, 354, 356 of the Bharatiya Nyaya Sanhita, 2023 (BNS)**, and **Sections 66E, 67, and 67A of the Information Technology Act, 2000** (dealing with privacy violations and obscene content), are analyzed in light of recent judicial interpretations. In *Manish Kathuria and Others v. State of Punjab and Others* (2001), the accused persistently sent obscene messages to a woman via email, highlighting the early onset of cyber harassment in India. *State of Tamil Nadu v. Suhas Katti* (2004) marked the **first conviction for cyberstalking under the IT Act**, showcasing prompt judicial response. In the *Sharmistha Mukherjee Case* (2017), a politician was targeted with morphed images, illustrating the political misuse of cyber abuse. *S. V. Shekar v. State* (2018) involved the posting of derogatory content about women journalists on Facebook,

[14] Chandrashekar AR, Nandini (2023) Crimes against women rise by 4%, cyber crimes increase by 11%: NCRB data. The News Minute. https://www.thenewsminute.com/news/crimes-against-women-rise-by-4-cyber-crimes-increase-by-11-ncrb-data
[15] Emili A. Vogels in The State of Online Harassment, published on January 13,2021, https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

underscoring the defamatory use of social media platforms and the need for better cyber accountability mechanisms.

1.2. Methodology

Since cyberstalking is a relatively recent phenomenon, studies have looked at cyberstalking when stalking moves to a new platform. Exploring some of the contributing variables behind conventional bullying is, therefore, necessary. This study employs a qualitative approach to examine the **effectiveness of legal responses to cyberstalking against women in India**, focusing on gaps within existing frameworks. The research is based on secondary sources, including judicial decisions, legal statutes, government reports, and scholarly articles. A case study method was used, such as the **Ritu Kohli case**, the first reported cyberstalking case in India, and the **Sharmistha Mukherjee case**, which involved political cyber harassment. A comparative legislative analysis evaluates how well provisions under the **Information Technology Act, 2000**, and the newly introduced **Bhartiya Nyaya Sanhita, 2023**, and **Data Protection and Privacy Act, 2023**, address such offenses. The aim is to assess whether the current legal tools are sufficient to deter and respond to cyberstalking crimes targeting women and to recommend focused reforms accordingly.

1.3 Aim of Study

The novelty of this study stems from its concurrent exploration of cyberstalking. The fact that their definitions overlap with victims' perspectives, risk factors, and outcomes, as well as the absence of a thorough examination of these related adverse behaviors, all support this cohesive framework.

- **Broader Aim:** The overarching goal of this study is to examine the prevalence and impact of cyberstalking against women in India while evaluating the effectiveness of current legal frameworks in addressing this issue.
- **Specific aims:**

➔ The first aim is to identify deficiencies within existing legal provisions, particularly those outlined in the Information Technology Act, 2000, the Bhartiya Nyaya Sanhita, 2023, and the Data Protection and Privacy Act, 2023.

➔ The second aim is to critically assess the role of law enforcement in tackling cyberstalking and propose legal reforms, cybersecurity measures, and strategies that victims can employ to counteract cyberstalking while enhancing women's digital safety.

1.4. Hypothesis

A. Cyberstalking is a growing menace in India, disproportionately targeting women due to gender-based vulnerabilities in the digital space.

B. Existing legal frameworks, including the IT Act, 2000, and the newly enacted laws, have significant loopholes in addressing cyberstalking effectively. For instance, while the IT Act, 2000, criminalizes identity theft and hacking, it does not comprehensively cover the non-consensual dissemination of personal information, a common tactic used by cyberstalkers. Similarly, Bhartiya Nyaya Sanhita, 2023, while incorporating provisions against stalking, lacks explicit definitions and procedural guidelines to tackle cross-jurisdictional cybercrimes effectively. These gaps necessitate urgent legislative amendments and improved law enforcement training to enhance the legal response to cyberstalking.

C. Increased awareness, legal reforms, and technological interventions can significantly reduce the prevalence and impact of cyberstalking on women.

1.4. Understanding Cyberstalking:

The use of electronic communication to follow someone, or persistent attempts to get in touch with someone to establish a personal relationship despite their obvious lack of interest,

is known as cyberstalking. Cyberstalking also includes monitoring the internet, email, or any other electronic communication.[16]

Stalking, in general terms, involves repeated acts of harassment directed at a specific individual, often creating fear or distress. Such behaviors may include persistently following the victim, making threatening or harassing phone calls, harming, vandalizing personal property, or leaving written messages and objects intended to intimidate. In some cases, stalking can escalate to severe violent acts, including physical harm, making it a serious offense that demands legal attention. The severity of the situation is largely determined by the stalker's pattern of behavior and intent. Cyberstalking, a modern extension of this crime, involves the use of digital platforms such as the internet, email, and other electronic communication tools to harass, intimidate, or threaten individuals, often blurring the boundaries between online and real-world threats.[17]

1.5. Modus Operandi of Cyberstalking

Cyberstalking manifests in various forms, each posing a significant threat to victims' privacy and security. ***Catfishing*** involves creating deceptive social media profiles, often mimicking real users with stolen images, to manipulate and exploit victims.[18] ***Tracking location check-ins*** enables stalkers to monitor an individual's movements through platforms like Facebook and Instagram, allowing them to analyze behavioral patterns. ***Virtual surveillance via Google Maps*** is another method where perpetrators use Street View or social media clues to determine a victim's surroundings.[19] ***Webcam hijacking*** is an invasive tactic where malware grants unauthorized access to a victim's webcam, violating their privacy. Similarly, ***stalkerware***, a covert form of spyware, discreetly tracks location, records conversations, and accesses personal data without detection.[20] ***Email stalking*** entails persistent, unsolicited messages containing threats, obscenities, or coercive attempts to initiate unwanted contact. ***Internet stalking*** extends this harassment to public forums, enabling slander and intimidation, sometimes escalating into real-world threats. Lastly, ***computer stalking*** occurs when perpetrators gain unauthorized control over a victim's device, forcing them to abandon their digital identity for safety. These cyberstalking methods underscore the urgent need for robust legal measures and cybersecurity practices to combat digital harassment effectively.[21]

1.6. The Vulnerability of Women in the Digital Space

It is as easy as pressing a button, cyberstalkers have no trouble finding their victims. Since they will conceal their identities, change important information, transfer and remove content in a matter of seconds, and destroy evidence, there is almost no chance that their actions will be questioned.[22]Women often divulge personal information to criminals or abusers because they trust them, which contributes to a high number of cybercrimes. Most of the time, serious crimes in cyberspace are also caused by the lack of platforms for filing complaints about

[16] https://cybercrime.gov.in/webform/crimecatdes.aspx
[17] Zero To Mastery In Information Security And Cyber Laws, by Dr. R.K. Jain, First Edition:2022
[18] Krasnova, K. A., & Kobets, P. N. (2019). *Cyberstalking: public danger, key factors and prevention*. *2*(2), 43–53. https://doi.org/10.31648/PW.3001
[19] Krasnova, K. A., & Kobets, P. N. (2019). *Cyberstalking: public danger, key factors and prevention*. *2*(2), 43–53. https://doi.org/10.31648/PW.3001
[20] https://www.geeksforgeeks.org/what-is-cyberstalking/
[21] https://www.geeksforgeeks.org/what-is-cyberstalking/
[22] Wan Rosli, Wan R., et al. "Mystalk Alert: A Response to Cyberstalking in Malaysia." (2022).https://bradscholars.brad.ac.uk/server/api/core/bitstreams/7e660fc9-fafa-4777-9ad0-2241a2e8a3b0/content

crimes.[23]Perpetrators exploit the anonymity of the internet to target victims repeatedly, the victim experiences feelings of irritation, abuse, emotional anxiety, and reputational damage.[24] Thanks to the internet, the ability to operate anonymously or under a pseudonym enables cyberstalkers to follow multiple victims from the comfort of their homes without ever leaving. According to a 2022 report by the National Crime Records Bureau (NCRB), cyberstalking cases have increased by 36% in the past five years, with over 70% of victims being women.[25] A study by the Internet Governance Foundation (2021) also highlights that 60% of female internet users in India have faced some form of online harassment, with anonymity playing a key role in enabling perpetrators to evade accountability.[26]

Additionally, gender influences the kinds of online harassment that people are likely to experience.[27]Studies on traditional and cyberstalking have shown that women are more likely than men to be stalked, suggesting that men primarily conduct these crimes against women for gender-motivated reasons[28]. When women voice their thoughts on contentious matters, they are frequently accused of "trespassing" or "invading" space reserved for men. This impression is particularly strong when female users share their thoughts in cyberspace.[29] Limited awareness among women about potential online risks and security measures increases their vulnerability. Justice delivery is hampered by legal framework flaws and shortcomings regarding cybercrimes against women, as well as delayed court proceedings.[30]

1.7 The Legal Framework in India

Both civil and criminal remedies are applicable within the legal framework for stalking in India. Sections 66A, 66E, and 72 read with Section 72A of the Information Technology (IT) Act, 2000, offer legal recourse for victims of cyberstalking. Section 66A (now struck down) criminalized the act of sending offensive messages online. Section 66E penalizes privacy violations through the capture, transmission, or publication of images without consent. Section 72 prescribes punishment for breaches of confidentiality and privacy by individuals with access to personal data. Section 72A extends liability to service providers who disclose information without consent, causing harm. Together, these provisions aim to address cyberstalking by safeguarding privacy and ensuring accountability for digital misconduct.[31]

---

[23]Kaur, A. (2025). Cybercrime Against Women in India: Challenges and Possible Solutions. *The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0*, 265-284.

[24] .Vidani, Jignesh, Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media (April 30, 2024). Available at SSRN: https://ssrn.com/abstract=4849744 or http://dx.doi.org/10.2139/ssrn.4849744 , Bhat, Rashid Manzoor, and Peer Amir Ahmad. "Social Media and the Cyber Crimes Against Women-A Study." *Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN* (2022): 2815-0953.

[25]https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf

[26] https://www.internetsociety.org/events/igf/2021/

[27] Emili A. Vogels in The State of Online Harassment, published on January 13,2021, https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

[28] Wan Rosli, Wan R., et al. "Mystalk Alert: A Response to Cyberstalking in Malaysia." (2022).https://bradscholars.brad.ac.uk/server/api/core/bitstreams/7e660fc9-fafa-4777-9ad0-2241a2e8a3b0/content

[29] Bhat, Rashid Manzoor, and Peer Amir Ahmad. "Social Media and the Cyber Crimes Against Women-A Study." *Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN* (2022): 2815-0953.

[30] .Vidani, Jignesh, Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media (April 30, 2024). Available at SSRN: https://ssrn.com/abstract=4849744 or http://dx.doi.org/10.2139/ssrn.4849744

[31] https://www.meity.gov.in/documents/act-and-policies/rules-for-information-technology-act-2000

The Bharatiya Nyaya Sanhita (BNS), 2023, introduces specific provisions to tackle offenses previously covered under the Indian Penal Code (IPC), 1860, particularly with regard to cyberstalking and crimes against women. Section 354D(1) of the IPC, which dealt with stalking, including harassment via electronic means, and prescribed imprisonment from one to three years along with a possible fine, corresponds to Section 354 in the BNS. Furthermore, acts causing grievous bodily harm during stalking incidents, once punishable under Sections 323 and 325 of the IPC, are now addressed under Sections 115(1) and 115(2) of the BNS. The definitions of 'voluntarily causing hurt' and 'voluntarily causing grievous hurt,' previously under Sections 321 and 322 of the IPC, are now incorporated within Sections 114 and 115 of the BNS. Assault, as described in Section 351 of the IPC, is now covered under Section 74 of the BNS. Public nuisance offenses, once under Section 268 of the IPC, are now addressed in Section 336 of the BNS. Sexual harassment offenses, which include physical contact, explicit sexual advances, and demands for sexual favors, formerly under Section 354A of the IPC, are now outlined in Section 63 of the BNS. Insults to a woman's modesty through words, sounds, or gestures, previously addressed by Section 509 of the IPC, correspond to Section 354 in the BNS. Finally, defamation, once dealt with under Section 499 of the IPC, is now covered in Section 356 of the BNS. These revisions within the BNS aim to provide a robust legal framework to combat cyberstalking and ensure the protection of women's rights in India.[32]

Offense	IPC Sections	BNS Sections	Description
Stalking (including cyber stalking)	354D	354	Punishment for stalking, including electronic communication harassment, with imprisonment of 1 to 3 years and a fine
Causing hurt	323	115(1)	Voluntarily causing simple hurt to a person
Causing grievous hurt	325	115(2)	Voluntarily causing grievous hurt to a person
Definition of voluntary hurt	321	114	Act done with intent or knowledge to cause hurt
Definition of voluntary grievous hurt	322	115	An act done with intent or knowledge to cause grievous hurt.
Assault or threat of violence	351	74	Intentionally causing another person to apprehend immediate violence.
Public nuisance	268	336	Any act causing common injury, danger, or annoyance to the public
Sexual harassment	354A	63	Making physical contact, showing pornography, or demanding sexual favors
Insulting a woman's modesty	509	354	Use of words, sounds, or gestures intended to insult a woman’s modesty
Defamation (including online harassment)	499	356	Publication of imputations harming a person's reputation

[32] https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

These legal changes highlight the Indian government's effort to create a more effective and detailed legal framework against cyberstalking, ensuring better protection and justice for women facing online harassment. The BNS provides clearer distinctions and stronger penalties for offenses, aligning with modern digital crimes. This transition underscores the necessity of adapting legal provisions to the evolving nature of cybercrimes, particularly against women, in India's rapidly digitizing society.[33]

The ***2001 case of Ritu Kohli*** starkly highlighted the growing menace of cyberstalking in India. When Mrs. Kohli approached the Delhi police to file a complaint against an anonymous stalker who inundated her with a series of threatening emails, the gravity of digital harassment came into sharp focus. The emails, which ranged from coercive demands to either appear naked for the perpetrator or pay him a sum of one lakh rupees, initially seemed ignorable. However, as the threats escalated, she became increasingly alarmed. Along with her details, including her home address and phone number, the stalker ominously threatened to share an altered photo of her online. Upon investigation, it was discovered that the image in question was one she had stored in her email account, thus confirming the stalker's intimate knowledge of her personal life. The situation worsened as she began receiving unsolicited phone calls from strangers requesting sexual favors at odd hours.

Following her complaint, authorities tracked the accused's IP address and uncovered that he had accessed Kohli's email account, revealing his access to her private photos. The accused, Manish Kathuria, was also found to have shared her phone number with other individuals while impersonating her in online chats. Ultimately, Kathuria pleaded guilty and was charged under Section 509 of the Indian Penal Code for insulting a woman's modesty, underscoring the need for more robust legal responses to such violations.[34]

State of Tamil Nadu v. Suhas Katti (2004), In this landmark case, Suhas Katti was charged with posting obscene, defamatory, and harassing messages about a woman in a public online forum. The victim, who endured significant societal pressure and emotional distress, filed a complaint, which ultimately led to Katti's arrest. The court convicted him under Section 67 of the Information Technology Act, 2000, and Section 509 of the Indian Penal Code. This case marked a significant milestone as the first cyberstalking conviction under the IT Act, reinforcing the urgent need for more stringent laws addressing digital harassment. Moreover, it showcased the legal system's capacity to navigate and adjudicate cybercrime cases, which often involve complex technological evidence and intricacies.[35]

The **Kalandi Charan Lenka v. State of Odisha, 2017,** highlights the grave repercussions of cyber stalking. The defendant exploited a female college student's name and photo to create a false Facebook account, published pornographic and altered photos, and sent offensive comments to her friends and contacts, impugning her character. Those messages came with sexual remarks and with the intent to harm the character and reputation of the victim. The messages not only affect the character of the victim girl but also encourage the other male members to have sex with the victim. The victim experienced tremendous psychological suffering and public humiliation after seeing those obscene messages. There was a feeling of trepidation. Inter alia to this, the accused pasted the pamphlet against the character of the victim girl on the hostel walls where she resides. The accused's conduct were deemed to be criminal impersonation and online harassment by the Orissa High Court. Sections 354A, 469, and 509 of the IPC and 66C and 66D of the Information Technology Act, were used to charge

[33] https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

[34] Manish Kathuria And Others vs State Of Punjab And Others on 10 September, 2014,https://indiankanoon.org/doc/38733736/ , https://www.bbc.com/news/world-asia-india-33532706

[35] Sharma, Nikita and Vadhera, Sakshi, Case Commentary : State of Tamil Nadu vs Suhas Katti (January 31, 2021). Available at SSRN: https://ssrn.com/abstract=3776961 or http://dx.doi.org/10.2139/ssrn.3776961

him. The ruling supported women's digital rights and privacy and reaffirmed the legal definition of cyberstalking. This case also serves as a reminder to society to be vigilant in the fight against cybercrime and to hold those responsible for such harmful activities accountable. It emphasizes the value of legal protections in the digital age and the need for constant efforts to ensure people's safety and rights.[36]

The historic instance of the stalking of former President Pranab Mukherjee's daughter, **Sharmistha Mukherjee Case (2017)**, was accused of being harassed by a guy and posting inappropriate or sexually explicit content on her Facebook profile. His daughter then complained to the Delhi police's cybercrime unit. To protect other victims, she decided to speak out against individuals who attempt to harass girls over social media.[37]

S. V. Shekar v. State (2018), The accused shared derogatory remarks against female journalists on social media. He was charged under Sections 4 and 6 of the Tamil Nadu Prohibition of Harassment of Women Act, 2002, as well as Sections 504 and 505 of the Indian Penal Code. Legal Implications: The case reaffirmed the legal penalties for gender-based online harassment and brought attention to the accountability of persons for offensive digital communication.[38]

1.9. Future Aspects of Combating Cyberstalking

Developing nations continue to be especially vulnerable because they frequently lack strong cybersecurity infrastructure. People in these areas are particularly vulnerable to crimes like phishing, identity theft, and disinformation because of a lack of resources and awareness of cyber threats.[39] The increase in cyberstalking necessitates a dynamic strategy to bolster legal and technological safeguards.(Bussu et al., 2023, #). Current laws are revised yet still lack a precise definition of cyberstalking, impose more severe fines, and expedite the settlement process. There are some ambiguities in cyber laws, especially about cyberstalking and its measurements. To combat this escalating threat, Bhartiya Nyaya Sanhita, 2023, should immediately include explicit rules on internet harassment. Campaigns for digital literacy that are specifically aimed at women must be supported to supplement these initiatives by increasing public awareness of online safety, reporting avenues, and privacy protection. Finally, because cyberstalking is a multinational crime, India has to strengthen its international collaboration with international cybersecurity organizations to make it easier to trace down, apprehend, and prosecute offenders.

1.10. Conclusion: Towards a Safer Digital Future for Women in India

In conclusion, this study has comprehensively analyzed cyberstalking, its legal redress, and the essential precautions to guard against such transgressions online. Cyberstalking is more than just an online annoyance; it is a serious security and privacy violation with real-world consequences. The increasing number of cyberstalking cases that target women in India highlights the pressing need for a multipronged strategy that includes societal, technological, and legal measures. As demonstrated by case studies like Ritu Kohli, Sharmistha Mukherjee, S. V. Shekar v. State (2018), Kalandi Charan Lenka v. State of Odisha and many more which

[36] https://indiankanoon.org/doc/73866393/ ,Kalandi Charan Lenka vs State Of Odisha on 16 January, 2017

[37] https://www.thehindu.com/news/national/President%E2%80%99s-daughter-Sharmistha-gets-harassed-on-Facebook/article14569500.ece

[38] S.V.Sekar vs The State Rep By Inspector Of Police on 14 December, 2018, https://indiankanoon.org/doc/176128508/ , https://www.thehindu.com/news/national/s-ve-shekher-case-sc-makes-it-clear-that-persons-who-forward-abusive-social-media-posts-cannot-shirk-liability/article67208819.ece , https://www.casemine.com/judgement/in/5e97ada94653d048ca2bf46e

[39] https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty#:~:text=Vulnerable%20populations%E2%80%93such%20as%20women,of%20authorship%20and%20intellectual%20property.

point to serious shortcomings in enforcement and judicial redress, existing frameworks—such as the IT Act, 2000, and the Bhartiya Nyaya Sanhita, 2023—remain insufficient in addressing the complex and multifaceted nature of digital harassment. According to this article, developing a secure digital. This paper asserts that creating a secure digital space for women is the collective responsibility of all stakeholders.

A thorough plan is essential. India can greatly improve case resolution by strengthening legislative provisions with clear definitions of cyberstalking and providing law enforcement with cutting-edge digital technologies. Extensive awareness efforts must be started simultaneously to inform women about their legal rights, reporting avenues, and internet safety. Technology platforms must also be held responsible for preventing abuse and moderating material. To provide survivors with prompt assistance, victim support services, such as counseling and legal aid, should be increased.

Furthermore, establishing strong cooperation among law enforcement, legislators, and IT firms is essential to building a safer online environment. To combat cyberstalking, an integrated structure of responsibility, digital security, and legal efficacy is required. By implementing proactive measures, strengthening legal frameworks, and raising public consciousness, India can cultivate a more equitable cyberspace where women can engage freely and securely. Now, it is the era of meaningful action.

Disclosure of Competing Interests: The authors disclose no potential conflicts of interest regarding the research, writing, and publication of this paper.

References

1. Zero To Mastery In Information Security And Cyber Laws, by Dr. R.K. Jain, First Edition:2022
2. https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/LS10122024/2305.pdf
3. https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf
4. https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty#:~:text=Vulnerable%20populations%E2%80%93such%20as%20women,of%20authorship%20and%20intellectual%20property.
5. https://legislative.gov.in/constitution-of-india/ ,The Constitution of India
6. https://www.ncrb.gov.in/crime-in-india.html
7. https://indiankanoon.org/doc/127517806/ , Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018
8. Pande R. Virtual Reality and Real Threats: Gender Violence in a Digital Age.Current Research Journal of Social Sciences and Humanities. 2024 7(2). Avialable here: https://bit.ly/4a2vb6D
9. Rachna, and Rahul Varshney. 2024. “CYBERBULLYING AND CYBERSTALKING: BELONGINGS AND ANTICIPATION MEASURES IN INDIA”. *ShodhKosh: Journal of Visual and Performing Arts* 5 (1):1469–1476. https://doi.org/10.29121/shodhkosh.v5.i1.2024.4289.
10. Vyas Shivangi Anilkumar, & Dr. Prakashkumar Thakor. (2024). CYBER CRIME CYBERSTALKING THROUGH THE CYBER LAW FORENSIC SCIENCE AND CRIMINAL INVESTIGATION. *International Education and Research Journal (IERJ)*, *10*(6). https://doi.org/10.21276/IERJ24924152332304
11. Wan Rosli, Wan R., et al. "Mystalk Alert: A Response to Cyberstalking in Malaysia." (2022).https://bradscholars.brad.ac.uk/server/api/core/bitstreams/7e660fc9-fafa-4777-9ad0-2241a2e8a3b0/content

12. Kaur, A. (2025). Cybercrime Against Women in India: Challenges and Possible Solutions. *The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0*, 265-284.
13. .Vidani, Jignesh, Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media (April 30, 2024). Available at SSRN: https://ssrn.com/abstract=4849744 or http://dx.doi.org/10.2139/ssrn.4849744 , Bhat, Rashid Manzoor, and Peer Amir Ahmad. "Social Media and the Cyber Crimes Against Women-A Study." *Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN* (2022): 2815-0953.
14. https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf
15. Halder, Debarati and Jaishankar, K., Cyber Victimization in India: A Baseline Survey Report (2010) (December 1, 2010). Available at SSRN: https://ssrn.com/abstract=1759708 or http://dx.doi.org/10.2139/ssrn.1759708
16. https://www.internetsociety.org/events/igf/2021/
17. Bhat, Rashid Manzoor, and Peer Amir Ahmad. "Social Media and the Cyber Crimes Against Women-A Study." *Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN* (2022): 2815-0953.
18. Krasnova, K. A., & Kobets, P. N. (2019). *Cyberstalking: public danger, key factors and prevention*. *2*(2), 43–53. https://doi.org/10.31648/PW.3001
19. https://www.geeksforgeeks.org/what-is-cyberstalking/
20. https://www.meity.gov.in/documents/act-and-policies/rules-for-information-technology-act-2000
21. https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
22. Manish Kathuria And Others vs State Of Punjab And Others on 10 September, 2014,https://indiankanoon.org/doc/38733736/ , https://www.bbc.com/news/world-asia-india-33532706
23. Sharma, Nikita and Vadhera, Sakshi, Case Commentary : State of Tamil Nadu vs Suhas Katti (January 31, 2021). Available at SSRN: https://ssrn.com/abstract=3776961 or http://dx.doi.org/10.2139/ssrn.3776961
24. https://www.thehindu.com/news/national/President%E2%80%99s-daughter-Sharmistha-gets-harassed-on-Facebook/article14569500.ece
25. S.V.Sekar vs The State Rep By Inspector Of Police on 14 December, 2018, https://indiankanoon.org/doc/176128508/ , https://www.thehindu.com/news/national/s-ve-shekher-case-sc-makes-it-clear-that-persons-who-forward-abusive-social-media-posts-cannot-shirk-liability/article67208819.ece , https://www.casemine.com/judgement/in/5e97ada94653d048ca2bf46e
26. Bussu, A., Ashton, SA., Pulina, M. *et al.* An explorative qualitative study of cyberbullying and cyberstalking in a higher education community. *Crime Prev Community Saf* 25, 359–385 (2023). https://doi.org/10.1057/s41300-023-00186-0
27. https://indiankanoon.org/doc/73866393/ ,Kalandi Charan Lenka vs State Of Odisha on 16 January, 2017
28. Emili A. Vogels in The State of Online Harassment, published on January 13,2021, https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/