INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

A STUDY ANALYZING CURRENT LEGAL REMEDIES FOR CYBERSTALKING IN INDIA AND THEIR DEFICIENCIES

AUTHORED BY - GOSWAMI APEKSHA SUKHDEVPURI
Research Scholar
Affiliation: Gokul Global University, Siddhpur

CO-AUTHOR - DR ABHA SHARMA

Abstract

Communication can involve repetitive efforts by one individual to reach out to another, instilling a sense of threat in the latter. Cyberstalking has emerged as a worldwide concern and a growing societal issue. Addressing this challenge is complicated due to inadequate security technologies and a weak legal framework. There is an urgent need for research into the various aspects of cyberstalking to evaluate this social issue. This paper examines the issue of cyberstalking in India, along with relevant legal provisions that could aid in combating this problem. The study also highlights the shortcomings in India's legal framework. It relies entirely on secondary data. The findings indicate that while several legal provisions in India could assist in addressing cyberstalking, there are no direct laws specifically targeting this issue, and existing provisions contain numerous gaps. Therefore, taking preventative measures is the most effective approach, and it is essential to raise public awareness about the available solutions.

Keywords: Cybercrime, Cyberstalking, Cyberspace, Laws related to Cyberstalking

Introduction

Cyber stalking is a significant global concern and an increasingly prevalent social issue (Cyber Angels, 1999; Ellison, 1999; Ellison & Akdeniz, 1998; Report on Cyber Stalking, 1999), resulting in new perpetrators and victims (Wallace, 2000). It represents a modern method of stalking individuals within cyberspace, facilitated by advanced technology. The term "cyberspace" refers to the online environment where communication occurs via the internet.

ISSN: 2582-6433

Gordon Richard, Deputy Secretary of Defence in England, defines cyberspace as "a global domain within the information environment composed of the interconnected networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The European Commission provides another definition, describing it as "the virtual space in which electronic data circulate among computers worldwide."

Cyber stalking entails utilising electronic channels, such as the Internet, to stalk or harass individuals or groups. This can involve monitoring, making threats, vandalising, and defaming, as well as collecting information with the intent to intimidate and harass. It constitutes a crime where the assailant uses electronic communication methods—such as email, instant messaging (IM), or messages posted on websites or discussion forums—to harass the victim.

In cases of cyber stalking, an individual is pursued and pressured online by another person. This form of harassment instils fear and disrupts the victim's life. Cyber stalkers often engage in constant digital surveillance of their victims and may employ various unwanted tactics, including trolling, bullying, and sending threatening emails or messages. Typically, victims of stalking are targeted by ex-partners, family members, upset relatives, or envious colleagues.

In June 2000, the case of Manish Kathuria and Ritu Kohli emerged, marking it as the first instance of cyber stalking in India. Ritu Kohli was subjected to harassment by Manish Kathuria, who shared her phone number. This case was significant as it represented the first time in India where there was no direct interaction between the victim and the harasser, yet she received frequent calls from others incited by him. The unique nature of this case left both the police and the court uncertain about the appropriate laws to apply. Such situations can inflict severe harm on the mental well-being of the victim, and they can also disrupt the stability of their life. In this case, the police were able to trace the IP address of the sender and apprehended Prabhu a month later. However, in many instances, law enforcement does not assist the victims, leaving them feeling powerless. In August 2016, Sharmistha Mukherjee, the daughter of President Pranab Mukherjee, was stalked and harassed by an individual who posted sexually explicit content on her Facebook page and sent inappropriate messages through Facebook Messenger. Mukherjee shared screenshots of the messages she received and filed a complaint with the Cyber Crime unit of the Delhi Police.

ISSN: 2582-6433

Legislative Framework Governing Cyber Stalking in India

Currently, India lacks a distinct law that specifically targets cyber stalking. Instead, this crime is managed through an array of laws including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the Digital Personal Data Protection Act, 2023 (DPDP Act), and various constitutional rights. These regulations collectively outline substantive offences, procedural protections, evidentiary protocols, and safeguards for privacy relevant to incidents of cyber stalking.

1. Information Technology Act, 2000

The Information Technology Act, 2000 serves as the key legislation in India addressing cybercrime and electronic governance. Although it does not specifically mention "cyber stalking," several clauses are often utilised in cases of online harassment and digital mistreatment. Section 66C makes identity theft a criminal offence by penalising unauthorised use of someone else's password, electronic signature, or identification features. This is significant in situations where stalkers fabricate identities or gain unauthorised access to victims' online profiles. Section 66D penalises fraud by personation using computer resources and is typically invoked in scenarios involving fake social media accounts and online impersonation.

In addition, Section 66E offers protection against privacy violations by making it a crime to capture, publish, or share private images without consent. Sections 67 and 67A forbid the distribution or transmission of obscene and sexually explicit materials electronically, which is especially pertinent when cyber stalkers share personal images or abusive content to intimidate victims. Section 72 holds individuals accountable for unlawfully disclosing sensitive information acquired through electronic methods. Together, these provisions empower law enforcement to act against various forms of cyber stalking, despite the lack of a distinct statutory provision.

2. Bharatiya Nyaya Sanhita, 2023 (BNS)

The Bharatiya Nyaya Sanhita, 2023, which has succeeded the Indian Penal Code, offers substantial criminal provisions concerning cyber stalking. It criminalises behaviours such as stalking, criminal intimidation, sexual harassment, voyeurism, defamation, and anonymous threats when perpetrated through digital means. An individual who persistently reaches out to another person online, tracks their activities, sends threatening communications, or intimidates

ISSN: 2582-6433

them through electronic channels may face prosecution according to the relevant clauses of the BNS. Therefore, while the BNS does not include a dedicated section on cyber stalking, its provisions effectively tackle the criminal behaviour linked to online harassment.

3. Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)

The Bharatiya Nagarik Suraksha Sanhita, 2023 addresses the procedural dimensions related to the investigation and prosecution of cyber offences. It establishes the protocols for filing First Information Reports (FIRs), inquiring into cybercrime, detaining suspects, searching and seizing digital devices, gathering electronic evidence, and carrying out criminal trials. Given that cyber stalking cases frequently involve mobile devices, computers, cloud services, and social media data, the procedural protections outlined in the BNSS are crucial for facilitating fair and efficient investigations.

4. Bharatiya Sakshya Adhiniyam, 2023 (BSA)

The Bharatiya Sakshya Adhiniyam, 2023 updates the regulations pertaining to evidence by acknowledging electronic records as valid proof in court proceedings. This includes emails, WhatsApp conversations, text messages, posts on social media, surveillance footage, phone call logs, GPS information, screenshots, metadata, and other digital files, as long as they meet the legal criteria for authenticity and admissibility. Given that cyber stalking primarily occurs via electronic means, digital evidence frequently plays a vital role in achieving a conviction.

5. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 aims to safeguard individuals from unauthorised handling and exploitation of their personal data. It establishes guidelines regarding consent, legal processing, the duties of data custodians, data safety measures, and consequences for data violations. While this Act does not explicitly address cyber stalking as a criminal offence, it enhances the protection of victims by controlling access to personal data and minimising the chances for offenders to misuse such information.

Constitutional Protection

Cyber stalking has a direct impact on multiple Fundamental Rights guaranteed by the Constitution of India. Article 14 ensures equality under the law and equal protection of laws, meaning that victims are entitled to the same legal safeguards. Article 19(1)(a) protects freedom of speech and expression; however, such freedom does not extend to justifying online

ISSN: 2582-6433

harassment, intimidation, or defamation, as reasonable limits may be enforced under Article 19(2). Most significantly, Article 21 ensures the right to life and liberty, which encompasses the right to privacy, dignity, reputation, and mental health. The Supreme Court in Justice K. S. Puttaswamy (Retd.) v. Union of India affirmed that privacy is a fundamental right, thereby offering constitutional safeguards against unauthorised digital monitoring, cyber stalking, and the improper use of personal information.

Case study

1. *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

The landmark ruling in Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, was issued by a Nine-Judge Constitution Bench of the Supreme Court, which unanimously determined that the Right to Privacy constitutes a Fundamental Right safeguarded under Articles 14, 19, and 21 of the Constitution of India. While the case stemmed from a constitutional challenge to the Aadhaar Scheme, the Court thoroughly explored the dimensions of informational privacy, data protection, and individual autonomy in the context of the digital era. It acknowledged that advancements in technology have heightened the risks of unauthorised surveillance, misuse of personal data, and privacy invasions, thereby necessitating constitutional safeguards for personal information. This ruling carries profound implications for cyber stalking, as such offences entail persistent online monitoring, unauthorised tracking, hacking, the dissemination of private information, and digital harassment, all of which violate an individual's constitutional right to privacy. The Court underscored that privacy encompasses informational privacy and the authority over one's personal data, thus establishing a constitutional basis for the protection of victims of cyber stalking. This decision has emerged as a fundamental reference point for the interpretation of cyber laws, data protection statutes, and digital rights in India, ensuring that technological progress does not undermine the dignity and personal freedom of individuals.

2. Shreya Singhal v. Union of India, (2015) 5 SCC 1; AIR 2015 SC 1523

In the case of Shreya Singhal v. Union of India, (2015) 5 SCC 1; AIR 2015 SC 1523, the Supreme Court assessed whether Section 66A of the Information Technology Act, 2000 was constitutionally valid. This section made it an offence to send messages deemed "grossly offensive" or "annoying" via electronic means. The petitioner contended that this law was ambiguous, capricious, and often misapplied to curb legitimate speech on social media platforms. The Court determined that Section 66A infringed upon the fundamental right to

ISSN: 2582-6433

freedom of speech and expression as guaranteed by Article 19(1)(a), as its unclear language led to arbitrary detentions and did not meet the criteria for reasonable limitations outlined in Article 19(2). In abolishing Section 66A, the Supreme Court emphasised that real cybercrimes, such as cyber harassment, criminal threats, identity fraud, online slander, obscenity, and the distribution of sexually explicit content, can still be prosecuted under other sections of the Information Technology Act and criminal law. This ruling established a crucial equilibrium between upholding free expression and ensuring responsibility for improper behaviour online. It remains a significant reference point for dealing with cyber offences while preserving constitutional rights.

3. State of Tamil Nadu v. Suhas Katti, C. C. No. 4680 of 2004

The case of State of Tamil Nadu v. Suhas Katti, C. C. No. 4680 of 2004, adjudicated by the Chief Metropolitan Magistrate Court in Egmore, Chennai, is known as India's inaugural successful conviction regarding a cyber harassment incident. The defendant set up a fraudulent Yahoo! account under the victim's identity, disseminating vulgar and damaging messages on internet forums while misleading individuals to contact her for sexual services. Consequently, the victim endured a barrage of indecent calls and messages, resulting in significant psychological distress, humiliation, and harm to her reputation. The prosecution extensively utilised electronic evidence that had been gathered throughout the investigation process.

The Court found the accused guilty under Section 67 of the Information Technology Act, 2000, along with applicable sections of the Indian Penal Code at that time, concluding that the online dissemination of obscene and libellous content is a cybercrime subject to punishment. This ruling affirmed that electronic records are credible and can be used as evidence in criminal cases, illustrating that issues of cyber stalking and online harassment can be prosecuted effectively. This case serves as a pivotal reference in the evolution of cyber law in India and underscored the court's commitment to tackling crimes enabled by technology.

4. Kalandi Charan Lenka v. State of Odisha, 2017

In the case of Kalandi Charan Lenka v. State of Odisha (2017), the defendant allegedly established a counterfeit Facebook account using the victim's name, posted altered obscene images, and shared vulgar messages on social media intended to harass and slander her. The victim argued that these actions resulted in significant emotional turmoil, social shame, and irrevocable harm to her reputation. This case brought attention to the growing abuse of online platforms for stalking and targeting women.

ISSN: 2582-6433

The Orissa High Court denied the request for anticipatory bail, noting that cybercrimes involving false social media profiles, altered images, and persistent online harassment are serious offences that threaten a woman's dignity, privacy, and mental health. The Court stressed that law enforcement must treat such offences with urgency and seriousness. This ruling bolstered judicial acknowledgement of cyber stalking as a significant crime and highlighted the necessity for robust legal safeguards against harassment facilitated by technology.

Shortcomings of the Current Legislative Framework

Even though there are numerous legal provisions in place, the cyber stalking laws in India are plagued by various deficiencies. A primary issue is the lack of a specific legal definition and distinct offence for cyber stalking within the Information Technology Act, leading to dependence on various provisions found in different statutes. This fragmentation often results in ambiguity during the processes of investigation and prosecution.

Another considerable hurdle is the fast-paced evolution of technology, which allows offenders to mask their identities through the use of virtual private networks (VPNs), encrypted messaging, pseudonymous accounts, and anonymous online platforms. Consequently, pinpointing the culprits becomes technically challenging and requires significant time. Cyber stalking often involves perpetrators situated outside of India, giving rise to international jurisdictional complications that hinder investigations, evidence acquisition, and the process of extradition.

The overall efficacy of the legal framework is further diminished due to a lack of adequate cyber forensic resources and a scarcity of skilled professionals. Numerous police departments do not have dedicated cybercrime units, specialised digital forensic labs, or the necessary technological know-how to address advanced cybercrimes. Prolonged delays in receiving information from social media platforms and internet service providers also extend investigation timelines, diminishing the likelihood of attaining successful convictions.

Victims encounter numerous practical challenges as well. The issue of under-reporting is prevalent, as many individuals avoid coming forward due to fears of social repercussions, retaliation, damage to their reputation, or a lack of faith in law enforcement. Current legislation offers minimal immediate protection for victims, such as emergency restraining orders, online protection orders, identity safeguarding, or access to psychological support. Additionally,

ISSN: 2582-6433

electronic evidence is vulnerable and can be easily modified, deleted, or encrypted if not quickly preserved, creating further obstacles for those investigating these crimes.

Finally, there is a significant gap in public awareness surrounding cybersecurity and legal options. Many internet users lack knowledge about privacy controls, mechanisms for reporting incidents, best practices for digital safety, or the legal protections available to them. The prevalence of insufficient cyber literacy exacerbates the rising rates of cyber stalking and undermines the effectiveness of the existing legal protections in place.

Conclusion

Cyber stalking presents a significant threat to individual privacy, dignity, and safety in the age of technology. India has established an extensive legal system through the Information Technology Act of 2000, the Bharatiya Nyaya Sanhita of 2023, the Bharatiya Nagarik Suraksha Sanhita of 2023, the Bharatiya Sakshya Adhiniyam of 2023, the Digital Personal Data Protection Act of 2023, and constitutional provisions under Articles 14, 19, and 21. Together, these laws create avenues for investigating and penalising different types of cyber stalking. Nevertheless, challenges such as the lack of a specific cyber stalking law, technological intricacies, issues with jurisdiction, insufficient cyber policing resources, delays in investigations, poor support for victims, and low levels of public awareness still obstruct effective law enforcement. Enhancing legislation, advancing cyber forensic capabilities, fostering international collaboration, boosting digital literacy, and offering improved protection and assistance for victims are crucial actions required to foster a safer and more secure digital landscape in India.