

Indian Journal of Modern Research and Reviews

This Journal is a member of the '*Committee on Publication Ethics*'

Online ISSN:2584-184X



Research Article

Cyber Stalking and Harassment of Women in India: A Legal Study

Dr. Prahalad ^{1*},  Dr. Ravinder Kumar ², Gurpreet Singh ³

¹ Associate Professor, Department of Legal Studies, IEC University, Baddi, Himachal Pradesh, India

² Associate Professor, Sri Sukhmani College of Law, Derabassi, Punjab, India

³ Research Scholar, Department of Legal Studies, IEC University, Baddi, Himachal Pradesh, India

Corresponding Author: *Dr. Prahalad

DOI: <https://doi.org/10.5281/zenodo.21308910>

Abstract

Due to the increasing growth of digital communication mediums in India, there has been a steep surge in the cases of cybercrime against women in the form of cyber stalking and online harassment. This paper analyses the adequacy of the laws which regulate such offenses, i.e., the adequacy of Information Technology Act, 2000 and the Indian Penal Code, 1860, which has been amended through the Criminal Law (Amendment) Act, 2013.

In addition to the above, the contribution of Indian higher judiciary towards the law has been reviewed with an emphasis on the inadequacies in the legal system. The study shows that despite some level of protection offered by the present legal regime, it lacks effectiveness in view of its gender neutrality, lack of definition, lack of procedural mechanism, and the inability to recognize the social context that exposes women to cybercrimes.

Manuscript Information

- ISSN No: 2584-184X
- Received: 04-04-2026
- Accepted: 27-05-2026
- Published: 30-05-2026
- MRR:4(5); 2026: 409-416
- ©2026, All Rights Reserved
- Plagiarism Checked: Yes
- Peer Review Process: Yes

How to Cite this Article

Prahalad, Kumar R, Singh G. Cyber Stalking and Harassment of Women in India: A Legal Study. Indian J Mod Res Rev. 2026;4(5):409-416.

Access this Article Online



www.mrrjournal.in

KEYWORDS: Cyber Stalking, Online Harassment, Women, Information Technology Act, Indian Penal Code, Cyber Law Reform.

1. INTRODUCTION

Jurist Salmond believed that the law is a tool used by the State to sustain an environment that facilitates order within society. Any drastic change that takes place in society calls for change in the existing legal framework. In the past three decades, we have witnessed the emergence of a digital revolution, which has brought about great changes. With the help of the internet, millions of people have been exposed to vast amounts of information, economic possibilities, and even ways to interact socially, making their lives more convenient than ever before. However, at the same time, this technology has made it easier for some to misuse it in order to threaten, intimidate, and muzzle women. Several cyber crimes have emerged within this period, and cyber stalking and harassment constitute two such grave crimes that pose serious threats not only in terms of frequency but also in terms of impact.¹

According to National Crime Records Bureau, there has been a sudden increase in the cases registered against the provisions of the IT Act, 2000 during a period of three years. There has been an increase in the numbers from 27,248 to 52,974, indicating almost a doubling of the figures within a three year span. Further, the statistics reveal that women have been victimized significantly under most of the categories of cybercrime. Crimes like cyberstalking, defamation and voyeurism have mainly targeted women, giving rise to gender specific cybercrimes.²

From a constitutional viewpoint, the courts consistently interpret Article 21 of the Constitution of India which guarantees the right to life and freedom of choice to include wider human entitlements. These include the right of dignity in living, protection from assault, and privacy, especially its educational aspect.³ The right to privacy was recognised as a fundamental right by the nine-judge Constitution Bench of the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India. The landmark ruling has bolstered the constitutional basis for protecting women against unwanted surveillance and constant digital bullying, which are often hallmarks of internet stalking.⁴ Wherein the law fails to protect against such forms of injury, the issue lies not merely in the absence of relevant legislation but rather constitutes a fundamental flaw within the constitutional structure itself.

The Information Technology Act, 2000, which provides the foundation for the Indian cyber law regime, was designed primarily to facilitate the development of electronic commerce and e-governance mechanisms. This law does not provide any provisions specifically dealing with or protecting against the injuries perpetrated in cyberspace on the basis of gender discrimination. While the courts have endeavored to fill in such lacunae in legislation through their innovative judgments in

cases such as Vishaka, there are limitations to judicial pronouncements under an inappropriate statute.⁵

2. Conceptual Framework: Defining Cyber Stalking and Online Harassment

It is essential to start any discussion on cyberstalking and cyberbullying with an appropriate definition of these concepts. Nonetheless, the lack of consistent terminology and clear definitions is a persistent issue within this field. One of the theories describing the behaviour of cyber offenders is known as the Space Transition theory proposed by Jaishankar. According to this model, people who would not commit crimes in their physical reality often find themselves motivated to do so in cyberspace. The primary reason behind the change is believed to be the anonymity of the virtual space, weak deterrence, and easy circumvention of jurisdictional boundaries.⁶

According to Halder and Jaishankar, cybercrimes against women are described as crimes committed against women, aiming to cause intentional harm to their mental and physical wellbeing via the latest advancements in communications technology, such as the internet and cellular telephones. This classification serves to underscore the sexual motive that characterizes cybercrimes against women, but fails to encompass the full ramifications on victims' personal, occupational, and financial lives.

In the bigger picture, cyber stalking and cyber threats⁷ is defined as the repetitive, unsolicited electronic tracking, harassing, threatening, or contacting of a person, usually a female, without their consent and without a valid reason, causing fear or anxiety in their mind. As stated by Yar, such behavior can be viewed as an age-old phenomenon in a brand-new technological environment, since even though stalking and harassment predates the advent of the internet, this medium has escalated the problem by erasing time and space constraints that existed in the past.⁸

"Online harassment is very much gendered," says Mary Anne Franks, who explains that the internet didn't create gender-based discrimination, it simply amplified and disseminated it. Digital contexts, she argues, provide offenders with new forms of domination and degradation that are not so readily available in offline contexts. She said the anonymity of the internet provides a discriminatory advantage, enabling people who

⁵ Vishaka and Others v. State of Rajasthan and Others, (1997) 6 SCC 241.

⁶ K. Jaishankar, 'Space Transition Theory of Cyber Crimes' in F. Schmallegger and M. Pittaro (eds.), *Crimes of the Internet* 283 (Prentice Hall, New Jersey, 2009).

⁷ Dr Ravinder Kumar, Navigating Intellectual Property Challenges in Cross-Border Data Transfer. (2024). American Journal of Public Diplomacy and International Studies (2993-2157), 2(7), 151-160.
<https://grnjournal.us/index.php/AJPDIS/article/view/5549>

⁸ Majid Yar, *Cyber Crime and Society* 9 (Sage Publications, London, 2006).

¹ Debarati Halder and K. Jaishankar, *Cyber Crimes Against Women in India* 3 (Sage Publications, New Delhi, 2017).

² National Crime Records Bureau, *Crime in India 2022* (Ministry of Home Affairs, Government of India, 2023).

³ The Constitution of India, 1950, Art. 21.

⁴ K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

might otherwise refrain from misconduct in real-life interactions because of social repercussions to engage in sustained online abuse with little fear of accountability.⁹

The term clear working classification is used in this analysis. Cyber-stalking is defined as the repeated activity of at least two times in which a person continues to pursue, peer, or try to contact another person through electronic communications without his or her permission. This behavior should be of a type that would reasonably lead the target to feel a threat to their safety or to cause substantial emotional distress to the target.

Online harassment, on the other hand, encompasses a broader spectrum of online behaviors. This not only covers stalking activities, but also threats, abusive or sexually explicit messages, circulation of degrading or defamatory material, sharing of intimate images without consent, collective abuse and encouragement or facilitation of others to engage in such actions online.

It's important to note that cyber stalking is not necessarily the same as online harassment because it's not the nature of the harassment that matters; it's whether the harassment happens continuously and repeatedly. Any communication or action that is offensive or threatening, even if serious, in and of itself is not stalking. The term "stalking" is defined by its repetitive and systematic nature and is a distinct category of behaviour from others, hence the severe psychological consequences for the victim.¹⁰

The Statutory Framework in India

3.1 The Information Technology Act, 2000 and Its Amendments

The Information Technology Act of 2000 was enacted primarily for granting legal sanction to electronic transactions and encouraging e-commerce development in India. Those provisions that relate to cybercrimes are grouped under Chapter XI, which has subsequently been substantially expanded via the Information Technology Amendment Act of 2008. While the Act includes aspects pertaining to cyber stalking and harassment within several sections, there is no particular provision made solely for these types of offenses. Thus, the entire legal framework seems to be rather disjointed and ineffective in this regard.¹¹

Clause 67 of the IT Act of 2000 prohibits publishing or transmitting sexually explicit matter or any publication that tends to corrupt or deprave anyone who comes across it. Clause 67 of the Act was used in cases of online harassment, especially when obscene material dealing with or containing depictions of women is posted. The clause was used in the case of State of

Tamil Nadu v. Suhas Katti, which was the first conviction under the IT Act.¹² The accused in this instance posted pornographic material on a Yahoo Group and provided the complainant's cell number in a manner which enabled him to make obscene telephone calls to her during the day and night. The speedy trial of a conviction for Sections 67 and 509 of the IPC in a relatively short period from the time of complaint to conviction served as an important precedent for the treatment of cyber harassment cases in a speedy and effective manner.

The provision of Section 66A of the Information Technology Act, which was added to the Act by the amendment in 2008, criminalized the sending of messages which are grossly offensive, threatening or false in electronic form. In reality it was one of the most often used provisions in offences of cyber stalking and online abuse, making it a cognisable offence which enabled the police to act without a court order. The language used within the provision was, however, very general and unclear, and eventually resulted in the constitutionality of the provision being deemed to be null and void. It was invalidated on the ground of its being too vague and liable to criminalise a large spectrum of speech protected by the Constitution in *Shreya Singhal v Union of India*.¹³ There was a gap in the law after Section 66A was repealed, and it has been poorly filled by any similar alternative provision.

Section 66C is about identity theft, which is punishable if someone uses a person's electronic signature or password or any other distinguishing identifying characteristic fraudulently or dishonestly. Section 66E, however, is concerned with the unauthorised photographing, publishing or dissemination of images of a person's private parts without his or her permission. While both provisions are applicable in some instances of cyber harassment (e.g., when the victim uses a fake online identity, or when intimate content is shared without their consent), both only apply to limited aspects of the overall range of behaviour constituting online harassment. Legal analysts have also noted that penalties under these sections may be inadequate to prevent the commission of such crimes.

Provisions on intermediaries (Section 79 of the Act) afford third-party content users on the intermediary's platform a kind of conditional immunity. This is a key part of the laws which govern accountability for cyber stalking and online harassment. An intermediary, having received information that it is hosting illegal content, has the risk of losing its safe harbour if it fails to act quickly to remove it, and may be liable for hosting it. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, have also added more obligations on the intermediaries to ensure that grievance redressal mechanisms are established and that the intermediaries acknowledge and respond to user complaints within a reasonable time limit.¹⁴ But the stated time limit of

⁹ Mary Anne Franks, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' 20 *Columbia Journal of Gender and Law* 224, 226 (2011).

¹⁰ The Information Technology Act, 2000 (No. 21 of 2000), s. 66A (struck down by *Shreya Singhal v. Union of India*, AIR 2015 SC 1523).

¹¹ Pavan Duggal, *Cyberlaw: The Indian Perspective* 87 (Saakshar Law Publications, New Delhi, 2nd edn., 2009).

¹² State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004.

¹³ *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

¹⁴ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (G.S.R. 139(E), 25 February 2021), Rule 4.

fifteen days for redressal of grievances appears to be clearly inadequate in cases where a woman is being subjected to continuous online stalking or harassment, as the harmful act continues unabated throughout the entire time taken for redressal.¹⁵

3.2 The Indian Penal Code, 1860: Pre-2013 Provisions

Prior to the introduction of the Criminal Law (Amendment) Act of 2013, the Indian Penal Code, 1860 used provisions that were initially created in relation to offline crimes while dealing with offences like cyberstalking and online harassment. Offences such as cyberstalking were covered by Section 509, which declared an act done with intent to outrage a woman's modesty to be illegal. While Section 503 dealt with criminal intimidation through threats against a person, his or her property, and reputation. Defamation was another cybercrime that fell within the ambit of Section 499 and Section 500 of the penal code. However, application of such provisions in the context of online crime was not simple because these provisions were created much earlier than the era of online communication through computers.¹⁶

This is shown by the case of *Manish Kathuria vs Ritu Kohli* which is one of the first cases in the Delhi courts that involve cyber harassment. In its attempt to solve an emerging problem using existing laws, the case showed the innovative nature of the judiciary, but it also revealed the need for new provisions. In the case of *Manish Kathuria*, the accused abused his victim through the misuse of her identity through online chat websites where he disclosed her contact information and took part in obscene chats using her identity, which resulted in obscene phone calls to her. Since there were no specific provisions dealing with such acts according to the Information Technology Act, the police applied Section 509 of the IPC. While the accused was convicted, the absence of any special provisions for cyber harassment meant that the process was unnecessarily complicated.¹⁷

The legal framework was not readily distinguishable as a separate offence in the context of stalking prior to the 2013 amendments. Stalking can be physical and online and involves repeated behaviour. It is the pattern of behaviour which is the wrongdoing not a single incident. The earlier provisions of the Penal Code were not designed to meet such conduct adequately. Individual acts might be too minor, taken in isolation, to merit criminal action, but cumulatively they formed a persistent pattern of harassment that had the effect of seriously intimidating and frightening the victim.¹⁸

3.3 The Criminal Law (Amendment) Act, 2013: Stalking and Related Offences

Criminal Law (Amendment) Act, 2013 was enacted after the 2012 Delhi Gang Rape incident and in the wake of the recommendations of the Justice J.S. Verma Committee represented a significant leap forward in terms of enhancing legal protection to women since Independence. The most significant revision for the reasons of this discussion was the inclusion of Section 354D of the Indian Penal Code which for the first time specifically outlaws stalking.

Stalking is defined as any repeated or unwanted action by a man towards a woman or an attempt by a man to establish unwanted contact with a woman, whether this is by means of the internet, the use of email or other form of electronic communications. This changed the legal landscape, making cyber stalking a clearly-defined offense and greatly broadening the definition of protection. Offence is cognisable on second and subsequent conviction and non-bailable in all cases. In this, it prescribes a punishment of up to three years' imprisonment as punishment for the first offense and up to five years imprisonment for the repeat offense.

The provision is a significant piece of legislation, but has been attacked for several reasons. Its narrow applicability is a major worry – it is restricted to situations in which the perpetrator is a male and the victim is a female, and it targets offenses that involve direct following or communication. This limited view misses the modern manifestations of cyber stalking, including covert (or ongoing) cyber surveillance in which no contact occurs. The second is that the claim of the victim has to be unambiguous, and this can be hard to establish, potentially shifting the blame back onto the victim, as earlier offenses have done.¹⁹

As per section 354A, introduced through amendment in 2013, sexual harassment is considered a criminal offense and covers actions such as making sexually colored remarks. Likewise, section 354C pertains to the crime of voyeurism and takes on particular importance when it comes to the surveillance or filming of women without their consent. As a whole, sections 354A, 354C, and 354D form part of the definition of criminal liability in cases of severe online harassment. Nonetheless, these sections still fail to form a cohesive legal concept when combined.²⁰

4. The Contribution of the Indian Judiciary

4.1 Early Judicial Engagement: Suhas Katti and Its Significance

The earliest and prominent judicial decision concerning cyber stalking and online harassment in India is in *State of Tamil Nadu v. Suhas Katti* (2004). The significance of the case goes

¹⁵ The Information Technology Act, 2000 (No. 21 of 2000), s. 79.

¹⁶ The Indian Penal Code, 1860 (No. 45 of 1860), s. 503.

¹⁷ *Manish Kathuria v. Ritu Kohli*, CC No. 14616/2014 (Delhi).

¹⁸ E.E. Mustaine and R. Tewksbury, 'A Routine Activity Theory Explanation for Women's Stalking Victimisations' 5(1) *Violence Against Women* 43, 47 (1999).

¹⁹ Talat Fatima, *Cyber Crimes* 54 (Eastern Book Company, Lucknow, 2016).

²⁰ The Indian Penal Code, 1860 (No. 45 of 1860), ss. 354A, 354C, 354D, 509.

beyond the actual verdict, as it also established a good template for dealing with cyber crimes. A complaint was immediately filed and with timely co-ordination between the cyber crime unit and the ISI, the investigation was resolved within a few days. The entire case was filed and finally convicted in a span of approximately seven months! This was quite rare in India at the time for a criminal case to be disposed of so quickly. The case highlighted that a useful mechanism to address cyber crime can be effectively established with effective institutional coordination and administrative support.

The case also helped to bring a certain legal clarity. It held that the information stored on electronic devices like records of subscribers and IP address records of service providers were admissible under the Evidence Act, 1872, as amended by IT Act. It also accepted that the publication of obscene material against a particular woman is being covered by Section 67 of the Information Technology Act and Section 509 of the Indian Penal Code. In addition to its legal impact, the speed of conviction instilled confidence in the effective implementation of cyber law and demonstrated its practical effectiveness in providing timely and real justice, which also had a deterrent effect.²¹

4.2 Intermediary Liability: Avnish Bajaj v. State

The first instance of a judicial pronouncement by the Delhi High Court in Avnish Bajaj v. State was on an important aspect relating to the criminal liability of online intermediaries with respect to the objectionable content posted by the user on its website. In the given case, there was the posting of a video clip on the website of Baazee.com which showed a student at school in an embarrassing condition, leading to the detention of the managing director of the firm and prosecution under Section 67 of the Information Technology Act. Upon looking into the ambit of intermediary liability, the Court came up with the pronouncement that a corporate head cannot be prosecuted without proper evidence that he had any knowledge of the offending content.²²

The question of intermediary liability is essential when considering ways to deal with cyberstalking and harassment. Most harassing content directed at women appears to be shared via major social networking sites, who may be considered as intermediaries in accordance with the Information Technology Act. This means that the intermediary's duty to remove such content and efficiency of notice-and-take down procedures become essential elements in assessing the efficacy of the law. The decision in Avnish Bajaj case, together with further developments in legislation, proved that safe harbor defense was not an absolute right and depended upon fulfilment of certain due diligence duties.

4.3 The Constitutional Dimension: Shreya Singhal and Its Aftermath

It is no wonder that the Supreme Court's decision in Shreya Singhal v. Union of India is considered to be one of the major decisions on cyber law in India. Section 66A of the Information Technology Act was struck down by a Division Bench of Justice R.F. Nariman and Justice J. Chelameswar on the basis that its language was not within the constitutional parameters of ensuring clarity of language when exercising the power of infringement of fundamental rights. "Grossly offensive" and "menacing in character" and "causing annoyance" were found to be too vague and left the provision open to arbitrary interpretation and enforcement. The Court established that on this basis, it is not consistent with Article 19(1)(a) of the Constitution.

Concurrently, the judgment has a multi-faceted effect to safeguard women against online abuse and cyber stalking. Section 66A had been used many times for online harassment of women as it allowed for prompt police action to be taken due to the message being deemed a cognisable offence. Its striking down was legally permitted but in doing so it left a noticeable gap in the legislative framework and this is yet to be effectively filled by a substitute provision. The larger lesson of Shreya Singhal is not that you cannot regulate online speech, but that you must do so with clarity of language, precision and with utmost respect for constitutional protections, as Section 66A did not.²³

The difference drawn by the court in the case of Shreya Singhal was a clear one between debate or advocacy on the one hand and incitement on the other. While it would be fair to say that the differentiation has been mostly in terms of freedom of speech, the lesson drawn from it can have crucial significance when it comes to any possible legislation pertaining to cyber harassment against women. The alternative to 66A should be drafted keeping the line intact.²⁴

4.4 Yogesh Prabhu and the First Cyber Stalking Conviction

Case of Yogesh Prabhu v State of Maharashtra is considered the first conviction in India on the charge of cyberstalking. In this case, the accused had made repeated threats to the victim by sending obscene and abusive messages to her via the Internet, despite the fact that she had made it clear to the accused that she does not want to communicate with him anymore. The cybercrime cell located the IP address of the messages and traced them back to the computer of the accused at his workplace. He was subsequently convicted of violating Section 509 of the Indian Penal Code, along with Section 66 E of IT Act, and sentenced to three years' imprisonment.²⁵

²¹ Prashant Mali, *Cyber Law and Cyber Crimes Simplified* 63 (Cyber Infomedia, Delhi, 2018).

²² Avnish Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427.

²³ S.K. Mohapatra, 'Victimisation of Women Under Cyberspace in Indian Environment' 2(3) *International Journal of Academic Research* 14, 16 (2015).

²⁴ Ajay Goswami v. Union of India, AIR 2007 SC 493.

²⁵ Yogesh Prabhu v. State of Maharashtra (Additional Metropolitan Magistrate, Mumbai, unreported, 2015).

Apart from its value as a precedent set by the court, this case draws attention to the methodologies employed while investigating cyber stalking cases. In this regard, identifying the defendant via Internet Protocol (IP) address tracing and immediate cooperation with the internet service provider to share information about the subscriber were key factors in forming an irrefutable line of evidence to prove the defendant's guilt. However, it should be noted that the ruling of the court revealed another issue in the legal system, namely, that despite all the evidence gathered, the defendant was charged under laws concerning the breach of privacy and insults towards a woman's modesty, which does not necessarily constitute cyber stalking.²⁶

5. Critical Assessment of Lacunae and Deficiencies

5.1 The Absence of a Comprehensive Definitional Framework

The primary deficiency in India's legislative response to cyber stalking and cyber harassment is the absence of clear definitions. While the IT Act, 2000 provides no specific definition for 'cyber stalking,' 'online harassment,' 'cyber bullying,' or 'cyber grooming,' neither does the term 'cyber space' have a legal definition in any statute. While Section 354D of the IPC attempts to regulate stalking, the section's scope is inadequate and fails to include all forms of online misconduct. Furthermore, the wording of the section presents problems with its implementation.

Failure to provide adequate definitions is a major problem with the law, going beyond mere theoretical issues. According to Fuller, in criminal law, the concept of legality requires that the definition of an offence be precise enough so that a common individual is aware of the proscribed behaviour, as well as preventing discretionary power in enforcing the legislation. Extending broad-based provisions intended to apply to offline conduct to online cases poses a challenge for achieving clarity and precision. In addition, the lack of legal definiteness goes against the mandate of Article 14 of the Constitution requiring laws to be reasonable and non-arbitrary.²⁷

5.2 The Post-Section 66A Lacuna

The repeal of Section 66A in 2015 has left a legislative vacuum which has yet to be adequately filled by any replacement legislation. Consequently, there is no distinct cognisable offence which specifically relates to the sending of threatening or highly offensive messages in electronic communications.

In such circumstances, the women who are repeatedly threatened or being harassed through social media or email generally have to rely on some general provisions such as

Section 503 of the Indian Penal Code (IPC), which covers criminal intimidation. But this must be backed up by evidence of actual threats to life, reputation or property. There may be behaviours that are harmful and persistently repeated and are not clearly covered by these legal definitions and so are not subject to punishment.

Where there is organised online harassment, that is, a number of people target a woman with abusive, threatening or degrading content, the situation grows even worse. While the effect of the overall campaign may be elusive and enduring, each attack may not be considered a criminal act on its own. At present, neither the Information Technology Act nor the Indian Penal Code expressly deals with such collective forms of online abuse. The law of criminal conspiracy (under Section 120B of the Penal Code) could potentially be applied, but is not commonly used in digital harassment cases.²⁸

5.3 Procedural and Enforcement Deficiencies

There are a number of procedural restrictions in the investigation and prosecution of cyber stalking and online harassment cases. Offences under the Indian Penal Code and the Information Technology Act are covered by the Code of Criminal Procedure, 1973, but this code was drafted for the traditional and physical crimes and is not always effective in addressing the challenges of digital crimes.

One such problem is the failure of the officer-in-charge of a police station to put the information on a police station record in writing of a cognisable offence as required by Section 154. This can cause difficulties for women reporting intimate cybercrime, as they may be expected to explain sensitive experiences to the officers tasked with investigating the crime, which may not be sufficiently trained in cybercrime investigations, and may not fully understand the psychological and social effects of intimate crimes.

There are also some technical issues with cyber stalking cases. The offender is typically identified by tracing electronic communications back to the device and then connecting the device to the person, an internet service provider may help with that. This requires in-depth expertise in the field of digital forensics, something not all police stations have, often only present in forensics units in larger towns and cities, and especially in cybercrime units. Victims in rural and semi-urban areas are thus often provided poor assistance, and this hampers the overall effectiveness of law enforcement.²⁹

Despite the formulation of the 2021 guidelines, the management of complaints about cyber-stalking and cyber-harassment remains a difficult undertaking. Most of the popular social media platforms are not located in India and they have been reluctant to cooperate with the Indian police when it comes to providing relevant user data or removing

²⁶ Vishwanath Paranjape, *Cyber Crimes and Law* 78 (Central Law Agency, Allahabad, 2010).

²⁷ Hemraj Saini, Yerra Shankar Rao and T.C. Panda, 'Cyber Crimes and Their Impacts: A Review' 2(3) *International Journal of Engineering Research and Applications* 202, 205 (2012).

²⁸ Julie Posetti et al., 'The Chilling: Global Trends in Online Violence Against Women Journalists' *UNESCO* 7 (2021).

²⁹ National Crime Records Bureau, *Crime in India 2020* (Ministry of Home Affairs, Government of India, September 2021), Chapter 18.

objectionable content. The lack of a data storage regulation makes it even harder. Furthermore, the architecture of most social media platforms that is geared towards maximizing user activity has at times played an active role in perpetuating cyber harassment, turning them into enablers rather than partners.³⁰

6. Reform Recommendations

Based on the above discussion, it is apparent that there needs to be a strategy for reforming this problem which is both narrow in scope and broad-based. Based on the above analysis, the following recommendations could be made in order to legislate and judiciously address this issue.

First of all, the legislature will have to bring about a particular legal provision which may either be in the form of an independent piece of legislation or may take the shape of a major amendment in the Information Technology Act. This law will have to provide a definition for the crimes of cyber stalking and online harassment as separate criminal offences. This definition must recognize the fact that stalking and online harassment is usually repetitive and organized and must incorporate all those cases where these acts are committed against a person without contacting him directly. In addition, it must also include the act of stalking and harassment in a clandestine manner without the knowledge of the individual concerned and collecting personal data about a person. Furthermore, the definition should be gender-sensitive in nature, as women tend to be particularly vulnerable to these kinds of crimes.³¹

Second, a new legal provision must be put in place in place of Section 66A. This should be more carefully worded to ensure that only communications aimed at causing reasonable fear of danger or serious psychological injury to another person may be penalised. Furthermore, the new law must clearly differentiate the prohibited actions from protected expressions. It must be noted that Shreya Singhal provides useful guidance in crafting a provision that is capable of passing judicial review under constitutional law.

Third, additional modifications to the Criminal Law (Amendment) Act, 2013 are needed, especially in Section 354D. First, stalking should not be limited to the direct contact between individuals. Digital surveillance, which does not require physical interaction between persons, should be included within its scope. Second, the criterion of a clear indication of disinterest should be modified or clarified. Third, the penalties for cyber stalking should be increased in cases of prolonged stalking and multiple offenders. Finally, extra care should be taken when handling cases involving former intimate partners, who account for a large percentage of victims.

Fourth, the legal framework of intermediary liability should be strengthened and have a clear and legitimate duty to respond

effectively to cyber-stalking and online harassment of women. The current system, relying mainly on individual victims reporting incidents of abuse, is inadequate when it comes to organised or multiple harassment on various platforms. Platforms should implement proactive measures to identify and remove illegal content and provide for strong sanctions for non-compliance to make it easier to implement in practice.

Fifth, the judiciary can take a proactive stance like it did in Vishaka and Others v. State of Rajasthan and Others if there is no legislation reform in the near future. If not, the Supreme Court set out standards for handling the situation of sexual harassment in the workplace where there was no law. This is similar to the procedures for cyber stalking and harassment cases and is an important temporary protection while a comparable set of guidelines for handling such incidents is being drafted.

Sixthly, special cyber-benches should be provided in High Courts and the Supreme Court. Cyber stalking cases are technically challenging, and therefore should be heard by judges who are IT knowledgeable, in information technology law. General courts may not have the expertise in electronic records, digital systems and forensic analysis that is necessary for such matters. Specialized courts for cyber offenses against women would provide more uniformity and precision in the delivery of justice, along with POCSO courts.³²

7. CONCLUSION

India's current legal system dealing with cyber stalking and online harassment of women reflects significant shortcomings. The main Act of Information Technology, 2000, is not specifically designed to prevent gender digital abuse and thus in practice is less effective at this goal. Section 354D was introduced in the Criminal Law (Amendment) Act, 2013, which was a step towards addressing the issue, but the definition of stalking is limited and does not adequately cover the more complex and expansive nature of online harassment in today's environment. While judicial activism such as Suhas Katti, Shreya Singhal and Puttaswamy has taken the discourse on digital rights a long way, the courts are still held back by the scope of current laws and can not provide the level of protection that any comprehensive law can offer.

Persistent online harassment has an impact on fundamental rights of life, personal liberty, equality, dignity and privacy which creates a positive obligation on the State to ensure meaningful legal protection. The inability to come with a proposal for a replacement for Section 66A, the inability to get Section 354D right, and the lack of rigor in the accountability norms for social media platforms all point to a failure to live up to this constitutional duty.

The proposed reform approach is feasible and based on existing legal principles. It is guided by the principles of the Constitution, the interpretation of higher courts and India's

³⁰ Adriana Rakshana, Sanaya Patel and Vandita Morarka,

'Safecity's Submission on Online Violence Against Women to the UN OHCHR' *Safecity* 21 (2018).

³¹ Council of Europe, Convention on Cybercrime, ETS No. 185, Budapest, 23 November 2001.

³² Sreekanth C. Nair v. Licensee/Developer, Crl. Rev. Pet. No. 2900 of 2008 (Kerala High Court).

international obligations. It will take legislation and judicial support for effective implementation. More crucially, it underscores that the digital realm is not a realm apart from constitutional governance, but one part of it – and that the rights of women must be contentiously respected and exercised in the same manner in the digital realm as in any other.

REFERENCES

1. Duggal P. *Cyberlaw: The Indian Perspective*. 2nd ed. New Delhi: Saakshar Law Publications; 2009.
2. Fatima T. *Cyber Crimes*. Lucknow: Eastern Book Company; 2016.
3. Fuller LL. *The Morality of Law*. Rev ed. New Haven: Yale University Press; 1969.
4. Halder D, Jaishankar K. *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations*. Pennsylvania: IGI Global; 2012.
5. Halder D, Jaishankar K. *Cyber Crimes Against Women in India*. New Delhi: Sage Publications; 2017.
6. Mali P. *Cyber Law and Cyber Crimes Simplified*. Delhi: Cyber Infomedia; 2018.
7. Paranjape V. *Cyber Crimes and Law*. Allahabad: Central Law Agency; 2010.
8. Reed C. *Making Laws for Cyberspace*. Oxford: Oxford University Press; 2012.
9. Yar M. *Cyber Crime and Society*. London: Sage Publications; 2006.
10. Franks MA. Unwilling avatars: Idealism and discrimination in cyberspace. *Columbia Journal of Gender and Law*. 2011;20:224.
11. Halder D, Jaishankar K. Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK and India. *Vict Offender*. 2014;9(2):234-253.
12. Jaishankar K. Space transition theory of cyber crimes. In: Schmallegger F, Pittaro M, editors. *Crimes of the Internet*. New Jersey: Prentice Hall; 2009.
13. Mohapatra SK. Victimization of women under cyberspace in Indian environment. *Int J Acad Res*. 2015;2(3):14-18.
14. Mustaine EE, Tewksbury R. A routine activity theory explanation for women's stalking victimisations. *Violence Against Women*. 1999;5(1):43-62.
15. National Crime Records Bureau. *Crime in India 2022*. New Delhi: Ministry of Home Affairs, Government of India; 2023.
16. Posetti J, et al. *The Chilling: Global Trends in Online Violence Against Women Journalists*. Paris: UNESCO; 2021.
17. Rakshana A, Patel S, Morarka V. *Safecity's Submission on Online Violence Against Women to the UN OHCHR*. Mumbai: Safecity; 2018.
18. Saini H, Rao YS, Panda TC. Cyber crimes and their impacts: A review. *Int J Eng Res Appl*. 2012;2(3):202-209.
19. Singh J. Violence against women in cyber world: A special reference to India. *Int J Adv Res Manag Soc Sci*. 2015.

Creative Commons License

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution–Non-commercial–No Derivatives 4.0 International (CC BY-NC-ND 4.0) License. This license permits users to copy and redistribute the material in any medium or format for non-commercial purposes only, provided that appropriate credit is given to the original author(s) and the source. No modifications, adaptations, or derivative works are permitted.