
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

**CYBER STALKING IN THE DIGITAL AGE: ASSESSING THE
EFFECTIVENESS OF THE BHARATIYA NYAYA SANHITA, 2023 AND
THE INFORMATION TECHNOLOGY ACT, 2000**

- Akanksha¹ & Dr. Poonam Choudhary²

ABSTRACT

The speedy development of information and communication technology has redefined how people communicate, interact and how they carry out day-to-day activities. Yet, the technology has prompted the emergence of cybercrimes, some of which have increasingly become the most widespread and threatening crimes, including cyber stalking. Cyber stalking is the systematic repetition of electronic communication technologies “such as social media, emails, and IM applications, to harass, intimidate, track or threaten a person. The crime is highly deterministic of privacy, dignity, reputation, and psychological health with women and young internet users as being the most susceptible ones. This has made cyber stalking more difficult to detect and prosecute due to its growing complexity by using artificial intelligence, counterfeit social media accounts, spyware, GPS tracking, and deep fake technology.

This research paper critically looks at the capability of the Indian legal system to deal with cyber stalking with specific focus on the Bharatiya Nyaya Sanhita, 2023 (BNS) and the Information Technology Act, 2000 (IT Act). It examines the definition, development, typologies and patterns of cyber stalking and the sufficiency of the current statutory frameworks in the fight against this fast-growing cybercrime. The paper also looks at major legal statements which have enhanced the privacy and digital rights protection, as well as pinpoint practical hurdles like technological progress, jurisdiction, poor cyber forensic framework, challenge of gathering electronic proofs and lack of reporting of crimes.

A doctrinal approach is applied in the research based on the evaluation of the statutes, judicial rulings, books, journal articles, and government reports among other secondary sources. It

¹ Research Scholar, Department of Law, M.M.H. College, Ghaziabad, Uttar Pradesh, India.

² Assistant Professor, Department of Law, M.M.H. College, Ghaziabad, Uttar Pradesh, India.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

ends by concluding that despite the fact that both the BNS, 2023 and the Information Technology Act, 2000 give a substantial legal basis into dealing with cyber stalking the current framework is incomplete and inadequate to be able to effectively respond to new technological threats. Some of the solutions advocated in the paper are thorough legislative reforms, acknowledgement of cyber stalking as a characterised crime, intensification of cyber forensic skills, committed training of law enforcement agencies, improved confrontations of victims, education of the masses, and enhancement of cross-national collaboration. Such policies are necessary to incorporate an effective legal framework that can protect privacy, dignity, and personal liberty as well as create a safer online space in India.

Keywords: Cyber Stalking; Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000; Cybercrime; Online Harassment; Digital Privacy; Electronic Evidence; Digital Forensics; Victim Protection; Cyber Law.

1. INTRODUCTION

Modern society has witnessed a revolution due to the fast development of information and communication technology that has allowed the free flow of information, e-business, e-learning, and social networking. Nonetheless, such technological advances have resulted in the development of advanced types of cyber crimes with one of the most frightening being cyber stalking. Cyber stalking is defined as the use of digital devices, namely social networks, emails, instant messaging programs, and other internet-based communications to harass, spy on, threaten, or intimidate another person. Cyber stalking offers criminals the chance to work anonymously, victims living geographically away, and cause lasting psychological, emotional and reputational damage, unlike the old-fashioned stalking that depends on matters that are not computerized (Kroll et al., 2017).³

In India, cyber stalking has increased astronomically with the rising use of internet and smartphones, and especially in the case of women, children, and other vulnerable individuals. With the implementation of the Bharatiya Nyaya Sanhita, 2023 to replace the previous Indian Penal Code, 1860, and the Information Technology Act, 2000 the government is showing its desire to better enforce the law against cyber offence. However, various obstacles that

³ Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* (2nd ed., LexisNexis 2019).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

interfere with proper enforcement include: the rise of technology, complexities of jurisdiction, lack of cyber forensic infrastructure and under-reporting.⁴

It is on this context that this paper critically reviews the legal framework that regulates cyber stalking in India by evaluating the efficiency of the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000. It also reports on the current legal and practical obstacles and suggests new or amendments to enhance the safety of people in the transforming digital space.⁵

2. MEANING AND EVOLUTION OF CYBER STALKING

Cyber stalking is a type of cybercrime whereby one person employs electronic communication technologies to harass, intimidate, threaten, spy on or communicate with another person against his/her will and induce fear, emotional distress or psychological comfort. It is an evolution of the old stalking in the virtual world where attackers capitalize on the anonymity, availability and worldwide connectivity offered by the internet to attack victims. Some of the common forms of cyber stalking are sending threatening or abusive emails and messages, creating fraudulent social accounts, stalking a victim, stealing his/her identity, hacking, and using spywares or GPS-tracking devices to trace the movements of a victim.⁶

Cyber stalking on the other hand is not limited by physical location or distance unlike in conventional stalking. Demonstrating that perpetrators may assault victims anytime and anywhere, the offence becomes less inquisitive and more tenacious. Some of the most vulnerable groups are women, children, journalists, celebrities, activists, and public authorities; however, every internet user can fall victim to them.⁷

The development of cyber stalking is strictly connected to the blistering development of internet and digital technologies of communication. In the early 1990s, the use of internet was only through emails and internet-based discussion boards where the very first cases of online harassment were announced. Cyber stalking has become more advanced with the introduction of social networking dependent sites in the early 2000s like Facebook, Instagram and subsequent messaging apps like WhatsApp and Telegram. Offenders started to use the fake

⁴ The Bharatiya Nyaya Sanhita, No. 45 of 2023; The Information Technology Act, No. 21 of 2000.

⁵ Farooq Ahmad, *Cyber Law in India: Law on Internet* (3rd ed., Pioneer Books 2021).

⁶ Farooq Ahmad, *Cyber Law in India: Law on Internet* (3rd ed., Pioneer Books 2021).

⁷ Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* (2nd ed., LexisNexis 2019).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

profiles, anonymous accounts, manipulation of the photos, and location-trackers to follow and stalk the victims.⁸

3. FORMS AND METHODS OF CYBER STALKING

The blistering development of online communication tools has allowed criminals to use technology to abuse its abilities in more sophisticated manners and cyber stalking is one of the most difficult cyber-crimes to solve and prosecute.⁹

3.1. Social Media Stalking

The most common type of cyber stalking is social media stalking. Offenders stalk users in the social networks (Facebook, Instagram) regularly. They can contribute to the unwanted messages, abusive messages, the creation of fake accounts, or recurring track of the victim online so that to cause fear or harassment.¹⁰

3.2. Email and Messaging Harassment

The emails, SMS, WhatsApp, Telegram or other messaging applications are often used by cyber stalkers to deceive the person with threatening, vulgar, defamatory or intimidating messages.¹¹

3.3. Fake Profiles and Identity Theft

The perpetrators will usually use the name and photos of the victim, or personal details to create a fake social media account. These counterfeit records are resorted to in order to obtain identity of the victim, misinformation and tarnished reputation.¹²

3.4. Online Surveillance and Monitoring

Cyber stalkers constantly spy on electronic activities of a victim tracking updates on social media platforms, browser history, location check-ins, shopping history and online footprints.¹³

3.5. GPS and Location Tracking

⁸ Pavan Duggal, *Cyber Law: The Indian Perspective* (3rd ed., Saakshar Law Publications 2020).

⁹ Pavan Duggal, *Cyber Law: The Indian Perspective* (3rd ed., Saakshar Law Publications 2020).

¹⁰ Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* (2nd ed., LexisNexis 2019).

¹¹ The Information Technology Act, No. 21 of 2000.

¹² Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing Co. 2017).

¹³ Farooq Ahmad, *Cyber Law in India: Law on Internet* (3rd ed., Pioneer Books 2021).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

The United States of America has modern technologies of smartphones and wearable devices that have GPS-enabling capabilities that can be used in stalking.¹⁴

3.6. Hacking of Online Accounts

Other frequent modes of cyber stalking include unauthorised access to victim email, social media, banking or cloud storage accounts.

3.7. Cyber Bullying and Public Defamation

Repeat of defamation statements, pornographic postings, gossips or certain embarrassing materials- Cyber stalkers might continuously post defamatory comments, sexually explicit content, rumors and embarrassing information about the victim on social media, blogs, or online forums. These will cause damage to the reputation of the victim and should isolate them socially.¹⁵

4. LEGAL FRAMEWORK GOVERNING CYBER STALKING IN INDIA

The statutory law that regulates cyber stalking in India includes the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology Act, 2000 (IT Act), and other related laws as a set aimed at penalizing crimes committed via digital platforms. No specific law exists that specifically addresses cyber stalking.¹⁶

4.I. Bharatiya Nyaya Sanhita, 2023

4.1.1. Section 78 – Stalking

Section 78 of the BNS outlaws stalking and identifies both physical and electronic stalking. It is the main law that prosecutes cyber stalking in India.¹⁷

4.1.2. Section 79 – Word, Gesture or Act Intended to Insult the Modesty of a Woman

Section 79 provides punishment to anyone who says statements, causes sounds or gestures, presents an object or interferes with the privacy of a woman, with the aim of insulting her modesty. Obscene or sexually explicit online communications, repeated indecent

¹⁴ Pavan Duggal, *Cyber Crime* (Saakshar Law Publications 2018).

¹⁵ S.K. Verma & Raman Mittal, *Legal Dimensions of Cyber Space* (Indian Law Institute, 2004).

¹⁶ The Bharatiya Nyaya Sanhita, No. 45 of 2023; The Information Technology Act, No. 21 of 2000.

¹⁷ The Bharatiya Nyaya Sanhita, No. 45 of 2023, Section 78.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

communications or online harassment through digital means can be subject to liability under this provision.¹⁸

4.1.3. Section 351 – Criminal Intimidation

Cyber stalkers are known to harass the victim by using emails, social network messages, or chat programs. These threats which are criminal intimidation in nature would be punishable by Section 351.¹⁹

4.1.4. Section 356 – Defamation

Posting defamatory or false images or content that misleads a victim online that is intended to harm the reputation may amount to defamation under Section 356.²⁰

5. INFORMATION TECHNOLOGY ACT, 2000

5.1. Section 43 – Unauthorised Access and Damage

Section 43 puts a civil liability on any individual who illegally enters a computer, computer network or computer resource or downloads, copies or extracts data with respect to a computer or a computer network.²¹

5.2. Section 66C – Identity Theft

This is a criminal provision that outlaws the use of electronic signature, password, digital identity or other distinguishing characteristics of another person with a fraudulent intent. It is usually used where offenders establish illegal online identities or defend themselves using an identity of a victim.²²

5.3. Section 66D – Cheating by Personation Using Computer Resources

Cyber stalkers may also play tricks on victims by opening fictional profiles or posing as a different individual on the internet. This misbehavior is punishable in Section 66D.²³

5.4. Section 66E – Violation of Privacy

¹⁸ The Bharatiya Nyaya Sanhita, No. 45 of 2023, Section 79.

¹⁹ The Bharatiya Nyaya Sanhita, No. 45 of 2023, Section 351.

²⁰ The Bharatiya Nyaya Sanhita, No. 45 of 2023, Section 356.

²¹ The Information Technology Act, No. 21 of 2000, Section 43.

²² The Information Technology Act, No. 21 of 2000, Section 66C.

²³ The Information Technology Act, No. 21 of 2000, Section 66D.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

Section 66E penalizes the deliberate act of capturing, publishing or transmitting images of a private part of a person without consent, therefore safeguarding the privacy of the victim against exploitation on the Internet.²⁴

5.5. Section 67 – Publishing or Transmitting Obscene Material

It is an offense (punishable by Section 67) to publish or transmit obscene content in electronic form. This is often applied in the cases of cyber stalking that entail obscene messages or the way of disseminating unpleasant digital content.²⁵

5.6. Section 67A – Publishing Sexually Explicit Material

Sexual material Publication or transmission of sexually explicit content via electronic media: This section punishable in 67A.²⁶

5.7. Section 67B – Child Sexual Abuse Material

In cases of cyber stalking of minors or any sexually explicit content that portrays children, the punishment is strictly in Section 67B.²⁷

5.8. Section 69A – Blocking of Online Content

The Central Government can ensure blocks on websites, applications or online materials that pose a risk to the state or are against the legal provisions. This authority can be utilized to eliminate illegal materials that are related to cyber stalking.²⁸

6. LANDMARK CASE LAWS

6.1. *Kalandi Charan Lenka v. State of Odisha*²⁹

Upon having his marriage proposal turned down, the alleged victim was repeatedly sent offensive text messages and defamatory emails by the accused, who went on to create a fraudulent Facebook account under her name and uploaded morphed nude photos, and consistently stalked her on the internet.

The Orissa High court noted that the claims posted online revealed they were being stalked, creating new social media profiles, committing identity theft, and sending obscene content

²⁴ The Information Technology Act, No. 21 of 2000, Section 66E.

²⁵ The Information Technology Act, No. 21 of 2000, Section 67.

²⁶ The Information Technology Act, No. 21 of 2000, Section 67A.

²⁷ The Information Technology Act, No. 21 of 2000, Section 67B.

²⁸ The Information Technology Act, No. 21 of 2000, Section 69A.

²⁹ *Kalandi Charan Lenka v. State of Odisha*, 2017 SCC OnLine Ori 1333.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

electronically. The Court was of the opinion that the prima facie was under Sections 354A, 354D, 465, 469, 506, 507 and 509 of the Information Technology Act, 2000 and Sections 66C, 66D, 67 and 67A of the Information Technology Act, 2000.

6.2. *State of Tamil Nadu v. Suhas Katti*

By using the name of the victim, the accused made a fake Yahoo account and sent obscene and defamatory messages online on groups, which caused constant online harassment.

The accused was found guilty of Collusion With the Intent of Fraud in Section 67 of the Information Technology Act, 2000 and applicable sections of the Indian Penal Code.³⁰

6.3. *Shreya Singhal v. Union of India*

Section 66A of the Information Technology Act, 2000 was questioned as being unconstitutional. The Supreme Court declared unconstitutional Section 66A in that it breached Article 19(1)(a) of the Constitution. According to the Court, terms of vaguity like grossly offensive and annoyance allowed arbitrary prosecution.³¹

6.4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*

Before the Supreme Court there was the question whether a basic right to privacy was guaranteed in the Constitution.

An eight member Constitution Bench in unison believed that the Right to Privacy is a basic right in Article 21 of the Constitution.³²

6.5. *Aveek Sarkar v. State of West Bengal*

The question that was presented to the Supreme Court was whether the release of some photographs was obscene or not. The Court embraced the present-day community standards test to ascertain obscenity.³³

6.6. *Sharat Babu Digumarti v. Government (NCT of Delhi)*

The Supreme Court reviewed whether there has been a connection between offences in Information Technology Act and Indian Penal Code on offences against electronic records.

³⁰*State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004 (Court of the Chief Metropolitan Magistrate, Egmore, Chennai, Judgment dated Nov. 5, 2004).

³¹*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

³²*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

³³*Aveek Sarkar v. State of West Bengal*, (2014) 4 SCC 257.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

The Court also made a decision that where an offence is conducted uniquely in respect to electronic records, and is advocated under the Information Technology Act, the special law customarily defeats the general provisions of the Indian Penal Code.³⁴

7. CRITICAL ANALYSIS OF THE EFFECTIVENESS OF THE BHARATIYA NYAYA SANHITA, 2023 AND THE INFORMATION TECHNOLOGY ACT, 2000

The passage of the Bharatiya Nyaya Sanhita, 2023 and the ongoing existence of the Information Technology Act, 2000 are the main legal measures of the Indian government to combat cyber stalking and other crimes carried out with the help of technologies. Although these legislations have legal acumen to prosecute criminals, they do not have the capacity of effectiveness because of the loopholes in legislation, technology and practical problems of enforcement.

7.1. Absence of a Specific Definition of Cyber Stalking

A key weakness of the current legal framework is the lack of a specific legal definition of cyber stalking. In spite of the fact that the concept of stalking is criminalized by Section 78 of the Bharatiya Nyaya Sanhita, 2023 that further prohibits monitoring the internet use of a woman, e-mail, or any other form of electronic communication, modern trends of cyber stalking through artificial intelligence generated deepfakes, GPS tracking, spyware, and cyber surveillance as well as impersonation via social media and constant online harassment on various digital platforms is not exhaustively included in this section.³⁵

7.2. Limitations of the Information Technology Act, 2000

Such offences as hacking, the theft of identity, the violation of the privacy, the cheating with the help of personation and the publication of obscene electronic content are the major offenses regulated by the Information Technology Act, 2000. Nevertheless, there is no offence listed separately, criminalising cyber stalking.³⁶

7.3. Effect of the Repeal of Section 66A

In *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, the Supreme Court held the provision of the Information Technology Act, Section 66A, as unconstitutional because it contravened the freedom of speech and expression. This ruling reinforced the constitutional safeguards against unreasonable criminalisation, but eliminated a clause that was often used by police to

³⁴ *Sharat Babu Digumarti v. Government (NCT of Delhi)*, (2017) 2 SCC 18.

³⁵ The Bharatiya Nyaya Sanhita, No. 45 of 2023, Section 78.

³⁶ Farooq Ahmad, *Cyber Law in India: Law on Internet* (3rd ed., Pioneer Books 2021).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

deal with abusive online messages. Since, police have been forced to base their position on alternative statutory provisions.³⁷

7.4. Difficulties in Investigation and Collection of Electronic Evidence

Even though electronic records are recognized as admissible evidence by the Bharatiya Sakshya Adhiniyam, 2023, they cannot be prosecuted effectively without the appropriate maintenance of screenshots, server logs, IP addresses, metadata, mobile devices and other digital forensic reports.³⁸

7.5. Jurisdictional Challenges

Cyber stalking often goes across national borders. A perpetrator can be based in a different State or even in a different country but attack individuals who are within India. Even though the Indian criminal law contains laws that deal with extra-territorial crimes, enforcement is usually slowed down by practice challenges associated with investigation, extradition, and mutual legal assistance, and collaboration with foreign online platforms.³⁹

7.6. Inadequate Cyber Forensic Infrastructure

The increased complexity of cyber crimes demands specific cyber forensic laboratories, trained investigators, digital forensic specialists as well as advanced technology infrastructure. Nonetheless, most police stations still find themselves short of skilled staff as well as up to date forensic laboratories.⁴⁰

8. CHALLENGES IN THE ENFORCEMENT OF LAWS AGAINST CYBER STALKING IN INDIA

Although there is the presence of the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, the successful implementation of the laws associated with cyber stalking is still a major challenge in India. Digital technology is a fast-changing phenomenon and the setup of probing and prosecuting culprits is usually hampered by legal, technical and institutional constraints. The key issues are discussed below.⁴¹

8.1. Absence of a Comprehensive Legal Framework

Even though the criminalization of stalking is contained in Section 78 of the Bharatiya Nyaya Sanhita, 2023, there is no special law or detailed statutory enactment that directly concerns

³⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

³⁸ The Bharatiya Sakshya Adhiniyam, No. 47 of 2023.

³⁹ Pavan Duggal, *Cyber Law: The Indian Perspective* (3rd ed., Saakshar Law Publications 2020).

⁴⁰ S.K. Verma & Raman Mittal, *Legal Dimensions of Cyber Space* (Indian Law Institute, 2004).

⁴¹ Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* (2nd ed., LexisNexis 2019).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

the issue of cyber stalking. This incoherent legal system can be very confusing during investigation and prosecution.⁴²

8.2. Rapid Technological Advancements

The rate at which technology is changing is outpacing laws. The use of artificial intelligence, encrypted messaging applications, anonymous accounts on social media, spyware, malware, and deepfake technology offers cyber stalkers an advantage as they can easily hide their identity along with harassing the victims. The current legislation tends to lag behind such advanced approaches.⁴³

8.3. Difficulty in Identifying Offenders

It is one of the greatest costs to detect cyber stalkers. Scammers often disguise themselves by using invalid identities, anonymous emails. Such methods complicate the tracking of the source of cyber attacks and identification of the offender by the law enforcement agencies.⁴⁴

8.4. Challenges in Collection and Preservation of Electronic Evidence

Effective prosecution requires effective gathering and maintenance of electronic proofs like emails, chat logs, screenshots, IP addresses, metadata, server logs, mobile devices, and social media communications. Digital evidence is very volatile and can easily be distorted, erased or destroyed. Poor forensic practices could affect the admissibility and credibility of evidence to courts.⁴⁵

8.5. Jurisdictional Issues

More often than not, cyber stalking is conducted between offenders, victims digital platforms and servers in various States or countries. These intercontinental crimes pose a jurisdiction issue and they necessitate international collaboration, via international treaties like the Mutual Legal Assistance Treaties, extradition agreements and liaison with foreign officials. These procedures tend to be time consuming and postponed investigation.⁴⁶

8.6. Inadequate Cyber Forensic Infrastructure

Despite the setting up of cyber forensic labs and cyber cells in India, a number of investigative agencies still experience a lack of skilled cyber professionals, purposeful forensic software, and technical infrastructures.⁴⁷

⁴² The Bharatiya Nyaya Sanhita, No. 45 of 2023, § 78.

⁴³ Pavan Duggal, *Cyber Law: The Indian Perspective* (3rd ed., Saakshar Law Publications 2020).

⁴⁴ Farooq Ahmad, *Cyber Law in India: Law on Internet* (3rd ed., Pioneer Books 2021).

⁴⁵ The Bharatiya Sakshya Adhiniyam, No. 47 of 2023.

⁴⁶ Pavan Duggal, *Cyber Crime: Prevention, Detection and Investigation* (Saakshar Law Publications 2018).

⁴⁷ Ministry of Home Affairs, Government of India, *Indian Cyber Crime Coordination Centre (I4C): Annual Report* (latest available ed.).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

8.7. Limited Capacity of Law Enforcement Agencies

The field of cybercrime investigations ought to be investigated by specialised knowledge of digital technologies, electronic evidence, artificial intelligence, and digital forensics. A lot of police officers are not provided with much technical training, which leads to inefficiency in terms of time required to carry out an investigation, the way they are able to collect their evidence, and the rate of convicting people declines.

8.8. Under-reporting of Cyber Stalking

Many cases of cyber stalking are not reported. Women especially fear social stigma, reputational injuries, victim-blaming, and a lack of trust in the criminal justice system, which prevents them and other victims of criminal activity, to reach out to law enforcement agencies.⁴⁸

9. SUGGESTIONS AND RECOMMENDATIONS

The rising nature of cyber stalking in India underscores the fact that a legal framework required is comprehensive and techno savvy. Even though the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 offer legal solutions, numerous legislative and technological interventions are required to curtail cyber stalking successfully by preventing, investigating and prosecuting it. It is suggested to take the following recommendations:

9.1. Enact a Comprehensive Law on Cyber Stalking

A special statute to deal specifically with cyber stalking should be enacted in India. Cyber stalking should be defined unambiguously in the law and adequately address emerging types of harassment in the online world, such as cyber surveillance, doxxing” location tracking, cyber bullying, deepfake technology, spyware, online impersonation, and artificial intelligence-based harassment.

9.2. Amend the Bharatiya Nyaya Sanhita, 2023

The BNS should be amended in section 78 to specifically cover the various types of technology-enabled stalking. This must also be rendered gender-neutral enabling all victims regardless of gender to enjoy equal protection of law. A stricter punishment should be proposed by the legislative body, in cases where cyber stalking causes severe psychological damage.

9.3. Strengthen the Information Technology Act, 2000

⁴⁸ National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2024).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

Amendments of the Information Technology Act with respect to cyber stalking should be carried out so that it is a stand-alone crime.

9.4. Strengthen Cyber Forensic Infrastructure

The Government must develop high level cyber forensic laboratory in all States and Union Territories with the modern digital investigation instrument.

9.5. Capacity Building of Law Enforcement Agencies

A cyberspace law Fire fighters, prosecutors, forensic experts and judges ought to undergo frequent specialised training on cybercrime investigation, digital evidence gathering, cyber forensics, artificial intelligence and international cyber laws.

9.6. Establish Specialised Cyber Stalking Units

Special cyber stalking investigative departments are expected to be developed in the cybercrime police departments to address any cases that relate to online harassment, identity theft, cyber surveillance and online sexual crimes.

10. CONCLUSION

The concept of cyber stalking has come out as one of the biggest cybercrimes of the digital age which is a great deterrent to the privacy, dignity, reputation and personal safety. The rising popularity of social media, smartphones and artificial intelligence has allowed criminals harass, spy on victims and threaten them with high-tech tools. Although India has reinforced their legal system by the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, the current laws are at best only partially operational in keeping up with the dynamic nature of cyber stalking.

This paper concludes that lack of an all-encompassing statutory definition of cyber stalking, scattered legal frameworks, technological progress, jurisdiction, deficient cyber forensic resources and underreporting are all obstacles to successful enforcement.

Hence the urgency in creating legislative changes which explicitly criminalize any cyber stalking (especially AI-enabled crimes), deepfakes, monitoring and surveillance online as well as impersonating another person over the Internet. Increasing cyber forensic capacity, specialised cybercrime units, social awareness programmes and international cooperation will increase the efficacy of the legal framework further. This collaboration of the legislature, judiciary, law enforcement agencies and technology companies with civil society is needed to achieve a safe digital environment and efficiently defend constitutional rights and freedoms of individuals in the digital age.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>