JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 22

Cyberstalking and the Enforcement Gap: Analyzing Legal Remedies and Procedural Hurdles in India

Amanpreet Kaur

CT University, Ludhiana

Recommended Citation:

Kaur (2026) "Cyberstalking and the Enforcement Gap: Analyzing Legal Remedies and Procedural Hurdles in India" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 22. (DOI)

ABSTRACT

The research paper critically evaluates the new criminal justice system which provides the framework to address the crime of Cyberstalking. The study analyses the shift of Section 354 of IPC to Section 78 of ***Bharatiya Nyaya Sanhita*** *(BNS) and the changes made under* ***Bharatiya Sakshya Adhiniyam (BSA), 2023****. While the law appears to be robust but in actual practice it's a 'paper tiger' and fails to ensure the proper justice due to 'Procedural Gaps'- like 'Attribution', Forensic backlogs, Evidentiary hurdles. Through the Doctrinal and comparative analysis, it is highlighted that the current law leads to the 'Secondary Victimization' by the way of seizure of personal devices in the process leading to 'Constitutional Failure'. While the failure in enforcement is the primary focus of the research paper, it cannot be studied in isolation without analysing the chain of gaps like gender -bias rules and provisions, technological lag of anonymity in AI-driven harassment, which ultimately results in the failure of the law. The paper concludes with the argument of transition from 'Paperwork to Practicality' through the possible modifications in the process like 'Digital Mirroring' policy and the cyber forensic labs etc. to ensure that the law can match the pace of digital crime.*

Keywords

Cyberstalking, Bharatiya Nyaya Sanhita (BNS), Digital Attribution, Section 63 BSA, Forensic Backlog, Secondary Victimization.

INTRODUCTION

Background

In the modern world, crime has shifted from streets to screens and one of them is Cyberstalking. Unlike traditional stalking, it is not limited to physical proximity or daylight but has risen to a 24/7 environment of fear. Legally, Section 78 of the Bharatiya Nyaya Sanhita (BNS), 2023, defines the offence as the act of monitoring a person's internet, email, or any form of electronic communication without their consent.[1] However, the modern law barely addresses the wide spectrum of digital harassment, which devoids the individuals of their right to access justice.

Imagine an individual seeking justice for the digital crime that took place against them, only to find out that they have to surrender their digital devices for years to get justice. This research identifies it as 'Digital Suicide' or 'Secondary Victimization' by the State. In K.S. Puttaswamy v. Union of India(2017), Right to Privacy under Article 21 was highlighted which gets violated by the very framework of law.[2] While the offender remains a 'Digital Ghost' protected from the burden, the victim suffers and practically gets punished by the very law which sought to protect them. This controversial reality is the underlying concept of the research.

Research Problem

In this research paper, the following questions are addressed:

A. Why have modernised laws failed to provide instantaneous remedies for crimes which take place in just seconds?

B. To what extent does the prolonged seizure of personal devices for forensic examination infringe upon the victim's Right to Privacy?

C. How do the statutory gaps in gender neutrality and technological scope fundamentally weaken the practical enforcement of Section 78 BNS?

Objectives of the Study

[1] Bharatiya Nyaya Sanhita, 2023, § 78,No. 45 of 2023, India Code (2023).
[2] *K.S. Puttaswamy v. Union of India,* (2017) 10 S.C.C. 1.

The main objective of the research work incline towards the Enforcement and the procedural hurdles that fails the law. This study aims to:

A. Evaluate the evidentiary hurdles under Section 63 of the BSA.
B. Critique the 18–24 month forensic backlog that causes the degradation of digital evidence.
C. Propose a shift from "Paperwork to Practicality" through decentralized forensic desks and "Digital Mirroring."

LITERATURE REVIEW

On the Exclusion of Non-Binary Identities

Although Section 78 of the Bharatiya Nyaya Sanhita (BNS), 2023, criminalizes stalking including Cyber stalking and digital monitoring but the legal lacuna of being gender -specific persists. The law only recognises the "Women" as a victim and the "Men" as a perpetrator.[3] Despite the *NALSA v Union of India* (2014) judgment , the law failed to keep the language gender – neutral.[4] Section 2(10) of the BNS recognises the 'transgender' community but fails to provide protection as Section 78 (Stalking) says: "Any man who follows a woman" the language remains gender – binary and hence , transgender persons are essentially legally invisible under this specific section.[5] The law provides **de jure** recognition to trans people but abandons them in **de facto** at same time.

Also, BNS without any substitute repealed the Section377 - IPC which was the only medium for the Trans people and men to file a complaint against the non consensual-sexual acts.[6] Hence, it violates the Right to Equality (Article 14) and Non-discrimination (Article 15) of the Indian Constitution. The Delhi High Court in *Gantavya Gulati v. Union of India* (W.P.(CRL) 2474/2024) highlighted the legal vacuum created because the government repealed Section 377 IPC without providing its alternative provisions.[7] Consequently, the significant demographic remains vulnerable and fails to get protection.

[3] Farhan Zia, *What do the New Criminal Codes Mean for Queer People?*, The Leaflet (July 7, 2024), *available at* https://theleaflet.in/criminal-justice/what-do-the-new-criminal-codes-mean-for-queer-people (last visited Apr. 11, 2026).
[4] *Nat'l Legal Servs. Auth. v. Union of India, (2014) 5 S.C.C. 438.*
[5] Saumya Uma, *Why the Bharatiya Nyay Sanhita Is a Missed Opportunity for Gender Justice,* The Wire (June 30, 2024), *available at* https://thewire.in/law/bharatiya-nyay-sanhita-women-gender-trans-queer-justice (last visited Apr. 11, 2026).
[6] Indian Penal Code, 1860, § 377, *repealed by* BNS, 2023.
[7] *Gantavya Gulati v. Union of India,* 2024 SCC OnLine Del 5990.

Technological Anonymity and AI

Today the use of AI has weaponised crime by deepfakes. Research from the Cyberpeace Foundation and Harvard Kennedy School (2023-2024) highlighted that the AI-generated materials are being used for blackmailing and defamation.[8] The real paradox is that of Attribution which means finding the true culprit behind the screen. The anonymity due to the use of VPNs and encrypting messages makes it difficult to find the perpetrators.

According to Kothari and Tibrewala (2024), the deepfakes act as 'Trojan Horse' in the Indian criminal system as it may appear to be true but hide the malicious intent and fabricated content.[9] The Bharatiya Sakshya Adhiniyam (BSA) 2023 has widened the scope of digital evidence but has a major lacuna in detecting AI-generated media as it has no required specific guidelines related to it. The court has no specific 'test' to prove that the content is fake or real. Therefore, it can mislead the jury or can hinder the proper functioning of Courts in providing justice.

The authors provide the Primary Recommendation which involves amending the Bharatiya Sakshya Adhiniyam (BSA) to include specialized protocols for AI-generated evidence, alongside a mandate for cryptographic watermarking to ensure evidentiary sanctity.[10]

Enforcement Gap

The Procedural disconnect fails the Cyber stalking laws. Under the Bharatiya Nagarik Suraksha Sanhita (BNSS) Section 173(1)(ii) allows victims to file an e-FIR so that there is procedural ease but law also mandates that FIR must be signed in person within 3 days.[11] This 72-hour window causes hurdles in the way of victims as many of them are often hesitant to file a complaint or the offender might use VPN to hide their identity. If the case is not signed within the stipulated time it remains "unregistered" and the offender gets plenty of time to delete the data which is volatile in nature. Moreover, after struck down Section 66A of IT Act in *Shreya Singhal v. Union of India* (2015) case, the police became more cautious about filing

[8] CyberPeace Foundation, *Cyberstalking: A Threat to Personal Privacy and Safety* (2024), *available at* cyberpeace.org (last visited Apr. 10, 2026); *see also* Belfer Center for Science and International Affairs, Harvard Kennedy School, *Technology Factsheet: Deepfakes* (2020), *available at* belfercenter.org. (last visited Apr. 10, 2026).

[9] Sanjana Kothari & Shaumya Tibrewala, *AI's Trojan Horse: The Deepfake Conundrum Under the Criminal Justice System,* 4 GLS *KALP: J. Multidisciplinary Stud.* 45 (2024), *available at* glskalp.in (last visited Apr. 10, 2026).

[10] Kothari & Tibrewala, *AI's Trojan Horse,* at 51.

[11] The Bharatiya Nagarik Suraksha Sanhita, 2023, § 173(1)(ii).

a case as high standards were prescribed in the case to ensure the protection of Free Speech.[12] The Police often take those messages as "annoyance" or "Online Spat" rather than a "Criminal Offence" and thus, many of the offences are not filed.

After the FIR is filed, the victim has to face an Evidentiary hurdle as the Section 63 of the BSA mandates that the digital message is only acceptable when it is Certified by a government- notified expert.[13] Section 63(4) of the Act provides that the certificate needs a signature from a "person in charge of the Computer or device" and a "designated expert".[14] The Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) ruled that the certificate is mandatory and cannot be skipped, making it a nightmare for the victims and acting as a shield indirectly.[15]

Digital Forensic Backlog is another unresolved issue. The wait time for a forensic analysis of a mobile device in major states ranges from 18 to 24 months. The problem is that digital data is 'volatile' and can be modified and if the technician checks that data after 2 years the evidence may become 'useless', 'stale' or 'technically unreadable'. According, the recent NCRB 'Crime in India' reports, the cybercrime registrations have surged (over 30% jump in 2023 alone), the conviction rate remains low (around 25% for cyber offences) primarily because trials are delayed waiting for these forensic reports.[16]

The final hurdle is of Attribution i.e. identifying and proving the specific individual behind the digital message. In India, Cyber-cells rely on "IPDR"(Internet Protocol Detail Records) and if the stalker uses VPNs or 'proxy servers' it turns out to be useless. Since companies like Meta are headquartered outside India, the police have to rely on long international legal processes (MLATs) to get user logs. As Aman Vedwal (2023) discusses how "Attribution" is the weakest link in Indian cyber-prosecution because the connection between the digital account and physical individual cannot be proven beyond reasonable doubt.[17]

---

[12] *Shreya Singhal v. Union of India,* (2015) 12 S.C.C. 73.
[13] The Bharatiya Sakshya Adhiniyam, 2023, § 63.
[14] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4).
[15] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* (2020) 7 S.C.C. 1.
[16] Nat'l Crime Records Bureau, Ministry of Home Affs., Crime in India 2023, *available at* ncrb.gov.in. (last visited Apr. 8, 2026).
[17] Aman Vedwal, Admissibility of Digital *Evidence* for Cyber Crime Investigation (2023), *available at* SSRN eLibrary (last visited Apr. 9, 2026).

Ultimately, India's current approach is towards procedural paperwork rather than substantive work of penalising criminals. These gaps need to be closed rather than abandoning victims in the legal world.

While the existing literature focuses on the multi-dimensional crisis in cyber stalking laws ranging from gender-bias to AI implications, this paper will focus specifically on Enforcement and Attribution Gap, as it is the most significant hurdle in obtaining a conviction under BNS and BSA.

While these authors identify the procedural gaps, there is a lack of deep analysis on how the new BSA certification rules specifically clash with the volatile nature of stalking evidence. This paper aims to fill that gap by examining the practical impossibility of attribution under the current framework.

RESEARCH METHODOLOGY

The research methodology adopted for this paper is primarily doctrinal, supplemented by a historical analysis of the transition from the Indian Penal Code (IPC) to the new criminal acts.

A. Doctrinal Analysis

The core of this study involves a "black-letter" analysis of the statutory text of the Bharatiya Nyaya Sanhita (BNS), 2023, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and the Bharatiya Sakshya Adhiniyam (BSA), 2023. This method is utilized to identify specific gaps regarding gender exclusion and digital evidence. A Doctrinal study is the most appropriate method to evaluate the potential legal challenges and loopholes of these laws which have been enacted recently.

B. Historical and Evolutionary Study

A comparative study between the repealed Indian Penal Code, 1860 and the BNS, 2023 is conducted to determine whether the new provisions introduced substantive reforms or is merely paperwork. This historical context is essential to understand the gender-binary logic in stalking laws (Section 78 BNS). The changes and modifications in Indian Evidence Act by BSA,2023 primarily deals with the digital Evidences which includes the Certification work and complexities. The major issue of AI generated content and Evidences and their admissibility is discussed in this research.

C. Data Collection and Sources

This research relies exclusively on secondary data.

Primary Sources: The official gazettes of the BNS, BNSS, and BSA 2023, along with landmark Supreme Court and High Court judgments, including *Gantavya Gulati v. Union of India* (2026) and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020). Secondary Sources: Peer-reviewed law journals e.g., Kothari & Tibrewala, (2024), Aman Vedwal, (2023), NCRB statistical reports.

THE IDENTITY CRISIS

To convict the offender, a significant task is finding that person and in the digital world it is the foremost legal challenge because the identity of the persons might remain 'Anonymous' because of the use of VPNs and Proxy Servers. Although Section 78 of BNS criminalises stalking, the practical problem is of 'anonymity' as it is difficult to connect the person's digital identity with the physical identity. If the law can't find and prove who sent the message or communicated digitally the law will subsequently fail. In the Manish Kathuria v. Ritu Kohli (2001) case, which was the India's first major case, the primary issue was just the 'Attribution' but the recent case of *State of West Bengal v. Animesh Boxi* (2018) shows now it's about deep-fake photos, encrypted cloud storage, and social media servers.[18] It also highlighted technical standards now required for conviction as the court relied heavily on digital forensics to link the accused to the unauthorized upload of private images. By comparing these two cases, it becomes clear that 'Attribution' is no longer just about identifying a phone number, but about proving a complex digital chain of custody that many local police stations are not yet equipped to handle.

The cyber stalkers steal the identity of others or create a fake one, committing a crime of 'Identity Theft' under Section 66C of IT Act,2000.[19] Therefore, Cyber Stalking is not just one crime of Stalking but of Identity Theft too. The Police finds it difficult to coordinate both in the investigation of the 'Double Crime' due to legal lacuna.

THE PAPERWORK TRAP

[18] *State of West Bengal v. Animesh Boxi,* G.R. Case No. 1287 of 2017, Tamluk District Court (2018).
[19] Information Technology Act, 2000, § 66C, No. 21.

The Challenge of Attribution is further complicated due to the technical paperwork required in the investigation under BSA, 2023. In this digital era, it has to be proved to judge that the message sent was authentic and to prove it the Section 63 of Bharatiya Sakshya Adhiniyam (BSA), mandates the 'Certification' of the Electronic Records by an expert.[20] In the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), Supreme Court under Section 65 now Section 63 ruled that the 'Certificate is Mandatory.'[21] Here the issue is that the victims generally have the screenshots of those messages and by the time they approach a lawyer related to Certification, the original message can be vanished as the digital data is volatile. The perpetrator gets sufficient time to remove that data online and gets the 'Benefit of Doubt' and without the Certification, the evidence is inadmissible.

The stalking usually happens on the Social Media apps like Instagram, WhatsApp or Twitter and headquarters of these big companies are outside of India and under the Information Technology (Intermediary Guidelines) Rules, these companies have to assist the Police during investigation.[22] To get the "Certificate" or "Log Files" from a US based Company the Indian police have to go through the Mutual Legal Assistance Treaty (MLAT) and this whole process took 6-12 months and by the time the data arrives the stalker might change their account or IP address and hence, it creates a 'Procedural Gap'.[23] This effectuates the idea that the law is only on paper which is not executed on time to protect the victims.

Another hurdle is that the victims themselves avoid filing the cases because they have to submit their digital devices to the police for investigation and due to the lengthy process of almost 1-2 years they withdraw the case rather than losing their devices to forensic labs.

THE FORENSIC BOTTLENECK

Section 176(3) of the Bharatiya Nagarik Suraksha Sanhita (BNSS) mandates forensic investigation for crimes punishable by 7 years or more but looks "illusionary" because the labs actually take 18-24 months to give the report. It gives the stalker a 'Free Pass' to continue the harassment. While in Hussainara *Khatoon v. Home Secretary, State of Bihar* (1979), the Court ruled that 'Right to Speedy Trial' is a part of Article21 of Indian

[20] The Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47.
[21] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1.
[22] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[23] Ministry of Home Affairs, Govt. Of India, *Comprehensive Guidelines on Investigation Abroad and Mutual Legal Assistance* (2019), *available at* mha.gov.in. (last visited Apr. 9, 2026).

Constitution, so making a victim wait for 2 years for a lab report is a clear Constitutional Breach.[24] Another case of *V.S. Rama Sarma v. State of Telangana* (2020) talks about the "chain of custody" as an essential tool.[25] If the device stays in a police station for months without being tested, the evidence can be tampered with or corrupted, and the stalker might get the benefit of doubt.

Why Cyber Stalking cases fail in Court?

Procedural Step Time	**Time Required**	**Victim's Concern**	**Legal Trap**
Evidence Seizure	Immediate	Police gain access to all private photos, chats, and bank details on the phone.	The victim chooses to delete the evidence to protect privacy instead of reporting.
Forensic Analysis	18–24 Months	Being without a smartphone for 2 years is socially and professionally impossible today.	The victim withdraws the complaint just to get their device back from the lab.
Global Data (MLAT)	6–12 Months	Have to explain the harassment multiple times to different authorities over a year.	Stalker remains free and continues the harassment during the long wait.
Trial Phase	3-5years	The victim loses interest or moves on with life, while the case remains stuck.	The "Chain of Evidence" is broken because witnesses or devices are lost over time

[24] *Hussainara Khatoon (I) v. Home Secretary, State of Bihar,* (1980) 1 S.C.C. 81.
[25] *V.S. Rama Sarma v. State of Telangana,* (2020) 10 S.C.C. 1.

The above table showcases how the enforcement gap is not the technical issue but a barrier for victims to choose between Justice and Privacy.

STRENGTHS AND WEAKNESSES OF THE CURRENT LAW

The new Section 78 of BNS is a modern and practical approach towards curbing the cybercrimes like Cyber stalking.[26] It underscores the 'online monitoring' and truly focuses on providing justice and taking into consideration the cybercrimes but at the same time it has some flaws because law appears to be a 'Paper Tiger' which looks scary and effective but fails in the practical approach when it comes to catching the perpetrators. The shift from IPC to BNS is notable in the criminal justice system but it didn't solve the 'Attribution Gap'. The Bharatiya Nagarik Suraksha Sanhita (BNSS) and BSA procedures which were not built for the speed of the internet are being complemented with BNS. The irony is that 21st century crimes rely on 19th century technological advancements and police infrastructure. The stalker can delete the message in just seconds while the police takes over weeks to just file a FIR correctly. It is a 'Strength-weakness paradox'. The BSA,2023 treats digital evidence as physical but ignores the fact that digital data can be changed or disappeared. While Section 63 mandates the certificate but doesn't provide any specialised tool to 'freeze' the account of the stalker immediately. Until the BNSS allows for 'Immediate Digital Seizure' without taking the physical device, the law will remain a 'paper tiger'.

PRACTICAL IMPLICATIONS

If we look practically, the law is failing not only because there is legal lacuna but the technicalities like Forensic lab reports delays, Certification and time taking process. The conviction rate is low which reduces the faith of victims in law. Another challenge is 'Secondary Victimization' where victims even after filing the complaint suffer because they have to submit their devices to the police not for days or weeks but for 1-2 years. In a modern economy where one's smartphone is essential for banking (UPI), work, and education, the state is asking the victim to commit 'digital suicide' just to report a crime. The law protects the anonymity of the stalker while putting the privacy of the victim at stake.

[26] Tarun, *A Critical Analysis of Cyber Stalking and Victimization of Women in India: Legislative and Judicial Approach*, 11 Nirma Univ. L.J. 49 (2022).

The Solution

The law is just ink on paper if it doesn't act in the real world. There is no advantage of writing laws if the laws do not deal with the time consuming and tiring technical processes.

A. There is a need for Cyber-Forensic Desks in every local police station which can verify the admissibility of screenshots. Every minor evidence is sent to over-burdened state labs, so decentralisation is needed at district level. This would ensure that 'Chain of Custody' is established within 72 hours and the critical evidence is not degraded.
B. The criteria of Section 63 BSA of Certification should be made less rigorous, simple and approachable that could be understood by the common people. Moreover, there should be 'Presumption of Authenticity" if the screenshots are being supported by the victim's affidavit. The 'Burden of Proof' should be shifted on the stalker to prove that they didn't send those messages.
C. There should be a 'Digital Mirroring' policy in which the stalking messages are copied or mirrored from the device afterwards the device should be returned and not put on a 2 years long wait. This would stop victims from withdrawing cases out of fear. The mirroring policy is already being used in high-level corporate fraud cases.[27] It should be mandatorily used in the cyber stalking cases where victims' privacy and property are both at risk.
D. There should be a 'Specialised Cyber Court' to deal with massive backlogs and to clear the cases not taking 2 years. The courts should be assisted with 'Technical Assessors' which can help the judges to understand the complex forensic reports.

CONCLUSION

Through this research, it can be concluded that India has made a significant notable move by marking a transition from IPC to BNS but it continues to remain a 'paper based' because in practical reality the law is not working as efficiently as it mentions in the provisions. While there are many loopholes in the law like gender-bias or AI deepfakes ,the Enforcement and Attribution Gap remains still unresolved. The research work shows that the 'digital ghost"- someone using VPNs or Fake IDs is impossible to catch if the police and administration do not work at the same pace with digitalised crimes.

[27] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

If the victims feel that the process of justice is more painful than the crime, they will avoid filing cases and hence, the law will lose its moral authority. The “Constitutional Failure” due to delay in Speedy Trial and technical process of Section 63 of BSA further imbalanced the law and Acts. The ‘Secondary Victimisation’ by the State from the e -FIR filing till submission of the digital devices makes victims vulnerable in the process of getting justice.

In summary, the government needs to transition from ‘Paperwork’ to ‘Practicality’. There is a requirement of the practical reforms like District-level forensic labs and Digital Mirroring that will ensure that the victim's privacy is protected and evidence is also preserved without the fear of erasure. Ultimately, the transition needs to be assisted with technological advancements because without proper cyber infrastructure the law will lag behind and will fail to provide justice as it will always remain a secondary priority of the procedural bureaucracy.

It is unfair to expect a cyberstalking victim to wait for years while forensic labs clear their backlogs. In the digital age, evidence is fragile and can be erased in an instant. If our courts and labs take years to respond to a crime that happens in seconds, then the system is failing. For these victims, justice delayed isn’t just a denial—it’s a total loss of their case.