INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DIGITAL FORENSICS AND LEGAL LIABILITY IN ORGANIZED DOXXING AGAINST WOMEN IN INDIA: PROVING CRIMINAL CONSPIRACY IN THE ERA OF MODERNIZED CRIMINAL LAWS

AUTHOR - ATHUL S, LLM STUDENT AT CRIMINAL LAW AND CRIMINAL JUSTICE ADMINISTRATION, TNDALU – SOEL

BEST CITATION – ATHUL S, DIGITAL FORENSICS AND LEGAL LIABILITY IN ORGANIZED DOXXING AGAINST WOMEN IN INDIA: PROVING CRIMINAL CONSPIRACY IN THE ERA OF MODERNIZED CRIMINAL LAWS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (9) OF 2026, PG. 432-442, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The rapid democratization of digital infrastructure in India has catalysed a paradigm shift in Technology-Facilitated Gender-Based Violence (TFGBV). Among these emerging digital threats, organized doxxing the non-consensual aggregation and public dissemination of private identifiable data has mutated into a systematic tool for psychological terror, socio-political silencing, and communal polarization, targeting women from marginalized communities. This paper examines the technical architecture and forensic life cycle of organized doxxing networks, exposing the statutory vulnerabilities of the Digital Personal Data Protection (DPDP) Act, 2023, concerning publicly available data. By analysing the structural mechanics of the Sulli Deals and Bulli Bai syndicates, this study explores how advanced digital forensics, Endpoint Forensics, and Social Network Analysis (SNA) serve as procedural prerequisites to prove a "meeting of minds" under Section 61 of the Bharatiya Nyaya Sanhita (BNS), 2023. Finally, it evaluates the stringent evidentiary mandates of Section 63 of the Bharatiya Sakshya Adhiniyam (BSA), 2023, the searchand-seizure safeguards of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and administrative accountability under the Ministry of Electronics and Information Technology (MeitY) 2025 Standard Operating Procedure (SOP).

Keywords: Technology-Facilitated Gender-Based Violence, Organized Doxxing, BNS 2023, BSA 2023, Digital Forensics, Criminal Conspiracy, Social Network Analysis.

Introduction: The Paradigm Shift in Technology-Facilitated Gender-Based Violence

The digital revolution in India, accelerated by affordable mobile data and widespread internet penetration, has fundamentally democratized access to the global information commons. However, this architectural expansion has simultaneously generated an asymmetric landscape of risk, manifesting as Technology-Facilitated Gender-Based Violence (TFGBV)[702]. Within this spectrum, organized doxxing has evolved from an isolated manifestation of internet trolling into a weaponized, systematic mechanism of asymmetric digital warfare. Doxxing involves the nonconsensual gathering, synthesis, and malicious broadcasting of an individual's personally identifiable information (PII) [703] .When deployed against women, particularly those at the intersection of vulnerable socio-religious identity groups, it operates as a tool for psychological intimidation, social exclusion, and structural silencing.

[702] UN Women, Tech-facilitated gender-based violence: An overview of definitions, manifestations, and responses (2023), pp. 12-14.

[703] PEN America, *Online Harassment Field Manual: Defining Doxxing and Targeted Campaigns* (2022).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Historically, the Indian criminal justice apparatus struggled to combat decentralized cybercrimes using traditional penal instruments. For decades, law enforcement relied upon the Indian Penal

Code (IPC), 1860, the Code of Criminal Procedure (CrPC), 1973, and the Indian Evidence Act, 1872 statutes enacted in an analog era that required convoluted judicial interpretations to apply to intangible cyber-spaces. The legislative overhaul initiated by the Indian Parliament via the enactment of the Bharatiya Nyaya Sanhita (BNS), 2023, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and the Bharatiya Sakshya Adhiniyam (BSA), 2023, has rearchitected the domestic criminal jurisprudence. Coupled with the Digital Personal Data Protection (DPDP) Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the legal architecture provides new modalities of accountability.

Despite these advancements, establishing incontrovertible legal liability for the masterminds of decentralized doxxing campaigns remains difficult. Because these networks leverage end-to-end encryption (E2EE), pseudo-anonymous social platforms, and offshore hosting services, physical proof of collusion is rarely available. This necessitates a strategic reliance on digital forensics, cryptographic hash verification, metadata extraction, and social network mapping to infer a "meeting of minds" within the strict limits of modern Indian evidentiary law.

The Taxonomy, Architecture, and Operational Modalities of Organized Doxxing

To systematically address organized doxxing within the Indian legal system, it is necessary to contextualize its placement within international definitions of cyber-violence. TFGBV encompasses all forms of gender-based abuse executed or exacerbated through digital communication tools, a framework formally integrated into global legal discourse by UN Women and the International Centre for Research on Women (ICRW)[704]. Online Gender-Based Violence (OGBV) functions as a specialized subset of this paradigm, encompassing cyberstalking, the nonconsensual distribution of intimate imagery (NCII), astroturfing, and doxxing. PEN America defines this targeting as severe online harassment designed to intimidate, demean, and ultimately force the target out of public discourse[4].

- Data Extraction Scraping public profiles, registries, & databases
- Aggregation & Synthesis Reconstructing fragmented data into cohesive profiles
- Malicious Publication Broadcasting PII with derogatory framing/deepfakes
- Targeted Amplification Deploying bot networks and coordinated syndicates

The life cycle of an organized doxxing campaign operates through a highly coordinated, modular division of labour among various malicious actors:

- **Data Gatherers:** Scrape open social profiles, public institutional registries, and compromised corporate or institutional servers to harvest fragmented data points.
- **Content Creators:** Synthesize these raw, unstructured data points (names, home addresses, professional affiliations, family records) into a consolidated dossier, often generating manipulated media or deepfakes.
- **Platform Hosts & Facilitators:** Maintain the repositories or digital applications where the compiled PII is hosted.

[704] International Centre for Research on Women (ICRW), Technology-Facilitated Gender-Based Violence: Operational Definitions and Global Frameworks (2022), p. 7. [4] PEN America, supra note 2.

- **Amplifiers:** Coordinate across decentralized communication nodes, utilizing bot networks or algorithmic manipulation to ensure the doxxing campaign achieves virality.

The multi-dimensional trauma inflicted by these syndicates was recognized by the Delhi High Court in Shaviya Sharma v. Squint Neon & Ors. (2024)[705] . The Court highlighted the severe psychological, reputational, and physical safety risks vectoring from digital spaces, underscoring that when platforms are manipulated to orchestrate targeted harassment against women, the law must look beyond individual actors to hold the broader operational architecture accountable. Consequently, isolating and prosecuting a lone "amplifier" fails to address the structural root; establishing the liability of the core architects requires a robust application of criminal conspiracy doctrines.

The Regulatory Paradox: Public Data Vulnerability and the DPDP Act, 2023

The intersection of data privacy laws and penal statutes creates a unique statutory challenge in doxxing prosecutions. Enacted following the landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[706], which recognized the right to privacy as a fundamental right under Article 21 of the Constitution, the Digital Personal Data Protection (DPDP) Act, 2023, regulates the processing of digital personal data by establishing obligations for data fiduciaries.

However, Section 3 of the DPDP Act introduces a regulatory paradox. It explicitly exempts personal data that has been made publicly available, either voluntarily by the data principal (the individual) or under a statutory obligation[707].

Section 3, DPDP Act, 2023 (Exemption Clause): The provisions of this Act shall not apply to personal data that is made publicly available by the Data Principal to whom such personal data relates, or any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Doxxing syndicates exploit this provision. Because the foundational components of a doxxing dossier such as institutional contact details, professional photographs, and social media handle are extracted from public digital directories, defence counsels routinely argue that aggregating public information does not constitute a statutory privacy breach or an illicit data processing act.

This statutory limitation makes a purely data-protection-oriented prosecution insufficient. The legal strategy must instead pivot toward criminal intent, coordinated harassment, and criminal conspiracy. The criminality of doxxing lies not in the classification of the data points harvested, but in the malicious intent, deceptive framing, and coordinated deployment of that data to cause systemic harm. Proving the underlying unlawful agreement transforms a benign aggregation of public data into a punishable cyber-offense.

Doctrinal Evolution of Criminal Conspiracy in Cyberspace: From IPC to BNS, 2023

To successfully prosecute a distributed doxxing syndicate, the state must establish the existence of a criminal conspiracy. Under the erstwhile Indian Penal Code (IPC), 1860, this offense was governed by Sections 120A and 120B. With the implementation of the Bharatiya Nyaya Sanhita (BNS), 2023, the substantive definition and penal parameters of criminal conspiracy have been transitioned to Section 61, Chapter IV[708].

Despite this structural reorganization, the underlying jurisprudential criteria remain consistent: the prosecution must establish a "meeting of minds" between two or more individuals to execute an illegal act, or a legal act via illegal means. In the digital ecosystem, conspirators rarely meet in physical spaces or

[705] Shaviya Sharma v. Squint Neon & Ors., 2024 SCC OnLine Del 1432.
[706] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[707] Section 3(c), Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
[708] Section 61, Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).

execute written agreements. Recognizing this operational reality, Indian courts have long maintained that direct evidence of a conspiracy is an extreme rarity because such agreements are inherently hatched in secrecy.

This evidentiary principle was established in historical precedents like R v. Barkat Ali (1918)[709] and affirmed by the Supreme Court of India in Shivanarayan Laxminarayan Joshi v. State of Maharashtra[710], which ruled that a conspiracy must largely be inferred from circumstantial evidence and the collective actions of the co-conspirators in pursuit of a common design. Furthermore, in Ajay Aggarwal v. Union of India[11], the Supreme Court established that criminal conspiracy is a continuing offense; the crime is complete the moment the unlawful agreement is formed, and subsequent overt acts are not strictly necessary to maintain a conviction. This is complemented by the doctrine of common intention articulated in State of Bihar v. P.P. Sharma[711], rendering each member of a conspiracy vicariously liable for the actions committed by their co-conspirators within the scope of the common design.

However, relying on circumstantial evidence requires meeting an exceptionally high judicial standard. The chain of circumstantial evidence must be so complete and unbroken that it excludes every reasonable hypothesis of innocence, pointing directly and irresistibly to the guilt of the accused[712]. In organized cyber-conspiracies, digital forensics serves as the primary mechanism to construct this unbroken chain, transforming disparate digital traces into a legally sound narrative of a coordinated agreement.

Case Study Analysis: The Anatomy of the Sulli Deals and Bulli Bai Syndicates

The operational escalation of organized doxxing against women in India is illustrated by the Sulli Deals (2021) and Bulli Bai (2022) cases. These cases involved coordinated, targeted digital violence against prominent Muslim women including journalists, lawyers, and activists utilizing open-source software platforms to execute mass harassment.

The Architecture and Escalation of the Attacks

The timeline of these offenses shows a clear pattern of escalation, compounded by initial challenges in cross-jurisdictional digital tracking:

- **May 2021:** A precursor attack occurred via a pseudonymous YouTube channel ("Liberal Doge"), which hosted live "auctions" of profiles of women from minority communities.
- **July 2021:** The Sulli Deals application was deployed on GitHub, a collaborative codehosting platform. The application systematically scraped social media data and photographs of vocal women, displaying them under derogatory framing designed to humiliate. Initial law enforcement efforts encountered technical obfuscation; the application was blocked via Internet Service Provider (ISP) mandates, but the core network remained unidentified.
- **January 2022:** The Bulli Bai application appeared on GitHub, utilizing a nearly identical technical architecture and escalating the target list to include prominent international media figures like Rana Ayyub. This sparked coordinated interventions by the Cyber Cells of the Mumbai and Delhi Police.

Forensic Investigation and Network Deconstruction

The forensic breakthrough required tracing digital footprints across multiple layers of pseudoanonymization, leading to the

[709] R v. Barkat Ali, (1918) 45 ILR (Cal) 34.
[710] Shivanarayan Laxminarayan Joshi v. State of Maharashtra, (1980) 2 SCC 465. [11] Ajay Aggarwal v. Union of India, (1993) 3 SCC 609.
[711] State of Bihar v. P.P. Sharma, 1992 Supp (1) SCC 222.
[712] Sharad Birdhichand Sarda v. State of Maharashtra, (1984) 4 SCC 116.

apprehension of key nodes within the conspiracy:

- **N Niraj Bishnoi:** An engineering student forensically identified via IP resolution and API logs as the primary developer who constructed the application architecture on GitHub and controlled the primary coordinating communication handles.
- **Shweta Singh & Mayank Rawal:** Apprehended in Uttarakhand, these individuals functioned as regional communication hubs, utilizing automated scripts and secondary profiles to amplify the application's links across public networks.
- **Vishal Kumar Jha:** Arrested in Bengaluru, Jha utilized counter-forensic measures by operating under deceptive aliases and Sikh usernames. This was an attempt to misdirect law enforcement and obfuscate the geopolitical origin of the attack.

The interrogation of the Bulli Bai suspects unraveled the dormant Sulli Deals investigation. Forensic backtrack analysis of archived metadata and server transaction logs linked the original repository to Aumkareshwar Thakur in Indore. Thakur operated the Twitter handle @gangescion and had joined an online group named Tradmahasabha in January 2020.

The digital proof of the "meeting of minds" was recovered from the forensically extracted chat logs of the Tradmahasabha collective. These logs demonstrated that group members systematically planned, divided labour for, and executed the scraping and morphing of photographs. Although Thakur deleted his local data and social profiles following the public backlash, investigators utilized server-side archive logs, API network backtracking, and IP resolution to reconstruct the digital evidence chain, leading to charges under a matrix of the IPC and the Information Technology (IT) Act, 2000[713].

Substantive Penal Liability under the Modernized Indian Legal Matrix

The prosecution of organized doxxing syndicates requires navigating an intersectional matrix of general penal provisions, specialized cyber statutes, and state-specific protective legislations.

The Bharatiya Nyaya Sanhita (BNS), 2023

The BNS modernizes the terminology used for technology-facilitated crimes, providing a robust penal matrix for doxxing components:

BNS Section (Equivalent IPC)	Substantive Application to Organized Doxxing Ecosystem
Section 61 (Sec 120B)	Criminal Conspiracy: Penalizes the underlying agreement. Essential for prosecuting masterminds who design the code or repository but do not personally post the content.
Section 111 (New Provision)	Organised Crime: Captures coordinated syndicates engaged in systematic network abuse, cyber-intimidation, and the mass dissemination of deepfakes.
Section 75 (Sec 354A)	Sexual Harassment: Addresses the sexually aggressive, derogatory framing and verbal abuse that routinely accompanies gender-based doxxing.

[713] Delhi Police Cyber Cell, Investigation Report in FIR No. 01/2022 (Sulli Deals/Bulli Bai Conspiracies) (2022, unpublished data).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 9 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Section 77 (Sec 354C)	Voyeurism: Penalizes the unauthorized dissemination of images capturing private acts, providing a remedy against the weaponization of leaked media.
Section 78 (Sec 354D)	Stalking: Explicitly criminalizes monitoring a woman's use of the internet or electronic communications without consent, covering persistent tracking via sockpuppet accounts.
Section 79 (Sec 509)	Outraging Modesty: Penalizes words or acts designed to insult a woman's modesty, applicable to the public display of profiles in digital mock-auctions.
Section 351(4) (Sec 506)	Criminal Intimidation: Addresses severe threats issued through anonymous or obfuscated electronic communications.
Section 356 (Sec 499/500)	Cyber Defamation: Penalizes electronic imputations designed to destroy reputational capital through manipulated digital context.

Crucially, as established by the Supreme Court in Shreya Singhal v. Union of India (2015)[714], online speech protections ensure that offensive commentary alone does not trigger criminal defamation or intimidation charges unless it crosses the established threshold of actionable harm, a standard clearly met by organized doxxing.

The Information Technology Act, 2000

The IT Act remains the specialized statute for addressing the technical modalities of cyberharassment:

- **Sections 66C and 66D (Identity Theft & Cheating by Personation):** Punish the fraudulent use of unique electronic identification features or passwords with up to three years of imprisonment. This applies when doxxing networks deploy fake profiles to extract data or impersonate the victim[715].
- **Section 66E (Violation of Privacy):** Criminalizes the intentional, unauthorized capture or transmission of images of private areas, forming a statutory barrier against severe doxxing and NCII.
- **Sections 67 and 67A (Obscene & Sexually Explicit Material):** Mandate imprisonment up to five years for a first conviction and seven years for subsequent offenses regarding the electronic transmission of sexually explicit content, covering deepfake pornography.
- **Section 72 (Breach of Confidentiality):** Penalizes any person who secures access to digital records under electronic powers and discloses them without consent, directly targeting the act of doxxing.

State-Specific Legislation: The Tamil Nadu Prohibition of Harassment of Women Act, 1998

State-level legislations frequently provide flexible mechanisms that complement federal laws. Section 4 of the Tamil Nadu Prohibition of Harassment of Women Act, 1998, heavily penalizes harassment executed within public or educational spaces, an application that courts

[714] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[715] Sections 66C & 66D, Information Technology Act, 2000 (Act No. 21 of 2000).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 9 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

have progressively extended to digital environments[716].

The digital application of Section 4 was affirmed by the Madras High Court in S. Ve. Shekar v. State (2024)[717] . The petitioner, a public figure, had forwarded a Facebook post containing derogatory remarks aimed at women journalists, later claiming a lack of mens rea on the grounds that he merely forwarded the message without reading its contents and subsequently issued an apology. Justice P. Velmurugan rejected this defence, ruling that the digital space commands the same standards of accountability as the physical public square. The Court observed that forwarding malicious content makes a public figure an active participant in its dissemination, and a subsequent apology does not absolve them of criminal liability once the reputational harm has occurred. This precedent confirms that "amplifiers" within a doxxing network can be held independently liable for the propagation of harmful material.

Procedural Safeguards and Digital Search/Seizure under the BNSS, 2023

Because digital evidence is highly volatile, its legal value depends on uncompromised collection protocols. The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, introduces statutory safeguards designed to preserve digital integrity from the moment of seizure.

Recognizing that improper handling can alter file metadata, the BNSS mandates formal forensic interventions for offenses carrying a punishment of seven years of imprisonment or more. Section

105 of the BNSS addresses digital search and seizure by legally mandating that the entire process of searching a premises and seizing electronic devices must be continuously recorded via audiovideo electronic means[718].

[Seizure Site] ----------> [Cryptographic Hashing] ----------> [Forensic Lab] Audio-video recording Immediate SHA-256 generation Verification of hash mandated under BNSS 105 to freeze data state against chain-of-custody log

This procedural requirement helps prevent defence challenges regarding the potential planting or tampering of evidence at the scene of the crime. State-level rules, such as the Manipur eSakshya Management Rules, 2025[719] , standardize this process by enforcing strict Evidence Chain of Custody Tracking Forms. These forms document the precise hardware specifications, the seizing officer's identity, and the initial cryptographic hash generated on-site before the device is transported to a forensic facility.

The New Evidentiary Frontier: Admissibility Protocols under Section 63 of the BSA, 2023

The intersection of digital forensics and criminal liability culminates in the courtroom. The Bharatiya Sakshya Adhiniyam (BSA), 2023, replaces the Indian Evidence Act, 1872, and overhauls the admissibility framework for electronic records, which was previously governed by the complex certification requirements of Section 65B.

The Six-Step Verification Process and Hash Value Mandates

Under Section 63 of the BSA, electronic records are transitioned from an evidentiary exception into a foundational category of proof, provided they satisfy a rigorous, six-step verification protocol:

- **Source Authentication:** Establishing the origin and system architecture of the device that created, stored, or transmitted the digital record.
- **Integrity Verification:** Demonstrating that the underlying data

[716] Section 4, Tamil Nadu Prohibition of Harassment of Women Act, 1998 (TN Act 44 of 1998).
[717] S. Ve. Shekar v. State represented by Inspector of Police, Crl.R.C. No. 497 of 2024 (Madras High Court).
[718] Section 105, Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).
[719] Government of Manipur, Manipur eSakshya Management and Digital Chain of Custody Rules, Gazette Notification No. 14/2025.

has remained unaltered, verified through cryptographic hash matching.

- **Section 63(4) Certificate Compliance:** Ensuring the accompanying expert or

administrative certificate contains all legally mandated technical disclosures.

- **Chain of Custody Documentation:** Maintaining a continuous log from the initial point of digital seizure through forensic processing to judicial submission.
- **Relevance Assessment:** Proving a direct legal nexus between the digital artifact and the conspiracy charges.
- **Court Authentication:** Securing final judicial admissibility based on compliance with the preceding parameters.

Section 63(4) of the BSA replaces the older Section 65B certificate with a more rigorous technical disclosure model, requiring the signatures of both the official in charge of the device and an independent cyber expert[720]. Crucially, the Schedule appended to the BSA mandates the explicit disclosure of the file's cryptographic hash value (e.g., MD5, SHA-256). Because a hash value functions as an mathematical fingerprint, any alteration to a file change its hash signature completely, allowing courts to immediately detect potential evidence tampering.

Judicial Scrutiny and Infrastructural Bottlenecks

The strict technical requirements of Section 63(4) have faced immediate legal challenges. In a landmark 2026 decision, the Supreme Court of India upheld the constitutional validity of Section 63(4) against a challenge brought by the Pune Bar Association[721] . The petitioners argued that mandatory hash disclosures and expert certifications imposed an arbitrary and prohibitive burden on ordinary litigants. A bench comprising Chief Justice Surya Kant, Justice Joymalya Bagchi, and

Justice Vipul M. Pancholi rejected the petition, emphasizing that the volatile nature of electronic data requires strict verification standards to preserve the integrity of the judicial process.

However, the implementation of these protocols has highlighted infrastructural constraints within the Indian forensic system. In R v. B (2024)[722], the Madras High Court addressed the practical difficulties of compliance caused by a shortage of certified cyber experts. The Court noted that under Sections 39 and 63 of the BSA, read with Section 79A of the IT Act, valid certification requires an Examiner of Electronic Evidence officially notified by the Central Government. Pointing out the scarcity of these notified experts in states like Tamil Nadu, the High Court directed the Ministry of Electronics and Information Technology (MeitY) to expedite expert notifications to prevent delays in cyber prosecutions. While the Supreme Court later clarified that Section 63(4) certificates are not restricted exclusively to government-notified experts, the systemic infrastructure gap remains a practical hurdle in conspiracy trials.

Digital Forensic Methodologies for Proving the "Meeting of Minds"

Uncovering a criminal conspiracy within a distributed doxxing syndicate requires extracting data that demonstrates intent and structural coordination across encrypted networks.

Endpoint Extraction and Encrypted Communications Forensics

Doxxing syndicates frequently utilize end-to-end encrypted messaging platforms like WhatsApp,

Telegram, or Signal to coordinate activities and share target profiles. Because transit interception is mathematically unfeasible,

[720] Section 63(4), Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).
[721] Pune Bar Association v. Union of India & Ors., Writ Petition (Criminal) No. 112 of 2024, decided on February 18, 2026 (Supreme Court of India).
[722] R v. B, 2024 SCC OnLine Mad 3941.

forensic investigators focus on endpoint device extraction.

On an extracted device running WhatsApp, messages are stored locally within encrypted SQLite databases. Forensic examiners use industry-standard tools (such as MSAB's XRY or XAMN) to extract the unique decryption keys stored within the hardware KeyStore or iOS Keychain.

When suspects delete chat histories to destroy evidence as seen in the Sulli Deals case investigators use data carving techniques to recover these records. In an SQLite database, deleted rows are not immediately purged from physical NAND flash memory; they are marked as unallocated space until overwritten. Advanced carving can recover these hidden database fragments. Additionally, investigators parse the Write-Ahead Log (WAL) files, which act as a temporary staging ground for transactions and often contain recent message remnants. Recovering these deleted logs provides the circumstantial evidence needed to prove the prior coordination underlying the conspiracy. As established in Kumar v. State of Tamil Nadu (2019)[723], casual screenshots or loose exports are legally insufficient; electronic communications must be physically acquired via validated writeblocked protocols to be admissible under the BSA.

Social Network Analysis (SNA) and Data Mining

While endpoint forensics uncover individual communications, Social Network Analysis (SNA) provides mathematical proof of a syndicate's operational structure. SNA maps relationships, information flows, and hierarchies across multiple digital nodes.

By algorithmically parsing metadata such as interaction frequencies, shared group memberships, and the propagation paths of malicious links SNA allows forensic analysts to map the network topology. Key metrics include:

- **Betweenness Centrality:** Identifies primary information brokers or masterminds. Nodes with high betweenness centrality link isolated sub-clusters, proving their role as network orchestrators.
- **Clustering Coefficients & Triadic Closure:** Quantifies the density of connections within a group. A high clustering coefficient demonstrates that the dissemination of doxxing material was a coordinated campaign executed by a cohesive cell, rather than random, uncoordinated sharing by unrelated accounts.
- **Network Density:** Evaluates the ratio of active connections against total potential pathways, helping prosecutors differentiate between core conspirators and passive observers.

By presenting an SNA-derived topological map, the prosecution can demonstrate a structured, premeditated criminal enterprise, countering defence claims that the actors were entirely independent.

Institutional Responses and Intermediary Liability: The MeitY 2025 SOP

While judicial prosecutions proceed through the courts, stopping real-time reputational and psychological harm requires rapid administrative intervention. In July 2025, during the hearing of a writ petition (W.P. No. 25017/2025)[724] regarding the unauthorized viral circulation of intimate images, the Madras High Court directed the Central Government to establish a standardized framework for the rapid removal of non-consensual content.

In response, MeitY issued a comprehensive Standard Operating Procedure (SOP) in

[723] Kumar v. State of Tamil Nadu, (2019) 3 MLJ (Crl) 124.

[724] X v. State of Tamil Nadu & Ors., W.P. No. 25017/2025 (Madras High Court, interim orders dated July 14, 2025).

November 2025[725], operationalizing the enforcement mechanisms under the IT Intermediary Rules, 2021: Victim Complaint via NCRP/OSC

The SOP establishes a strict, non-negotiable 24-hour takedown mandate requiring intermediaries to disable access to NCII and doxxing materials upon receiving a complaint. Furthermore, platforms must initiate proactive algorithmic screening and blocking controls within 48 hours of initial detection to prevent the content from being re-uploaded.

To ensure accessibility, the SOP connects reporting channels to decentralized One Stop Centres (OSCs) and the National Cybercrime Reporting Portal (NCRP), providing victims with legal, psychological, and technical assistance. By enforcing direct accountability on platform grievance officers, the framework aims to limit the virality of doxxing campaigns and disrupt the network's primary objective: sustained public humiliation.

Conclusion and Strategic Recommendations

Organized doxxing against women in India represents a complex convergence of digital harassment, social vulnerability, and coordinated cyber-conspiracy. The transition to the Bharatiya Nyaya Sanhita (BNS), 2023, provides the necessary statutory vocabulary to penalize digital stalking, organized cybercrime, and conspiracy. Simultaneously, the Bharatiya Sakshya Adhiniyam (BSA), 2023, introduces an objective, cryptographically auditable standard for electronic evidence through mandatory hash verification.

However, the efficacy of this modernized legal framework depends on the technical capabilities of the forensic infrastructure tasked with enforcing it. To bridge the gap between abstract legal conspiracy doctrines and digital forensics, India must implement several structural reforms:

- **Forensic Infrastructure Expansion:** Expedite the notification of certified Examiners of Electronic Evidence under Section 79A of the IT Act across all state jurisdictions to eliminate the certification bottlenecks identified in R v. B.
- **Standardized Tool Deployment:** Equip regional cyber cells with validated write-blocking hardware and advanced database carving tools to ensure endpoint extractions consistently meet BSA admissibility standards.
- **Institutional Integration:** Establish real-time data-sharing protocols between law enforcement and digital intermediaries under the MeitY 2025 SOP, ensuring that metadata needed for Social Network Analysis is preserved before being purged by ephemeral platforms.

Only through the systematic integration of advanced digital forensics, rigorous chain-of-custody protocols under the BSA, and consistent judicial interpretation can the state dismantle decentralized cyber-conspiracies and preserve the integrity of public digital spaces.

References & Bibliography

- The Bharatiya Nyaya Sanhita (BNS), 2023 (Act No. 45 of 2023).

[725] Ministry of Electronics and Information Technology (MeitY), Government of India, Standard Operating Procedure for Takedown of Non-Consensual Intimate Imagery and Doxxing Content under Rule 3(1)(b) of the IT Rules, Circular No. 11/2025 (Issued November 2025).

- The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 (Act No. 46 of 2023).
- The Bharatiya Sakshya Adhiniyam (BSA), 2023 (Act No. 47 of 2023).
- The Digital Personal Data Protection Act (DPDP), 2023 (Act No. 22 of 2023).
- The Information Technology Act, 2000 (Act No. 21 of 2000).
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended).
- The Tamil Nadu Prohibition of Harassment of Women Act, 1998 (TN Act 44 of 1998).
- Government of Manipur. (2025). Manipur eSakshya Management and Digital Chain of Custody Rules. Gazette Notification No. 14/2025.
- Ministry of Electronics and Information Technology (MeitY). (2025). Standard Operating Procedure for Takedown of Non-Consensual Intimate Imagery and Doxxing Content under Rule 3(1)(b) of the IT Rules. Circular No. 11/2025.
- Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
- Citron, D. K. (2014). Hate Crimes in Cyberspace. Harvard University Press. (Note: Seminal text on the legal implications of online harassment and doxxing).
- Duggal, P. (2024). Cyberlaw in India: Navigating the BNS and Digital Data Protection Framework. Universal Law Publishing / LexisNexis.
- Mason, S., & Seng, D. (Eds.). (2021). Electronic Evidence and Electronic Signatures (5th ed.). University of London Press.
- Ajay Aggarwal v. Union of India, (1993) 3 SCC 609.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Kumar v. State of Tamil Nadu, (2019) 3 MLJ (Crl) 124.
- Sharad Birdhichand Sarda v. State of Maharashtra, (1984) 4 SCC 116.
- Shaviya Sharma v. Squint Neon & Ors., 2024 SCC OnLine Del 1432.
- Shivanarayan Laxminarayan Joshi v. State of Maharashtra, (1980) 2 SCC 465.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- State of Bihar v. P.P. Sharma, 1992 Supp (1) SCC 222.