JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 2 (Apr.-Jun.) | 2026 Art. 03

Cyber Crimes In India: Legal Framework, Investigation Challenges, and Role of Electronic Evidence

Mohd Usman
Law Student, BA.LL.B. (Hons.),
Amity Law School, Amity University, Lucknow

Dr. Rohit Kumar Shukla
Assistant Professor,
Amity Law School, Amity University, Lucknow

Recommended Citation
Mohd Usman and Dr. Rohit Kumar Shukla, *Cyber Crimes In India: Legal Framework, Investigation Challenges, and Role of Electronic Evidence*, 2 JILPS 26-42 (2026).
Available at www.jilps.in/current-issue/

Cyber Crimes in India: Legal Framework, Investigation Challenges, and Role of Electronic Evidence

ABSTRACT

India's legal landscape has undergone a historic transformation with the transition from colonial-era legislations to the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA), operative from July 1, 2024. Against the backdrop of a 217% surge in cybercrime incidents between 2018 and 2023, this research paper provides an exhaustive analysis of the new framework designed to integrate technology into the Indian justice system. The study examines the substantive shifts in the BNS, particularly Section 111, which elevates cyber syndicates and "fraud factories" to the status of "Organized Crime," carrying severe penalties including life imprisonment. It further analyzes the codification of digital deception under Section 318 (Cyber Fraud) and the introduction of "Digital Sovereignty" offenses under Section 152. Procedurally, the paper evaluates the BNSS mandates, specifically the compulsory audio-video recording of search and seizure (Section 105) and the requirement for forensic expert visits at crime scenes (Section 176), highlighting the infrastructural deficits that threaten implementation. Furthermore, the paper critically assesses the evidentiary changes under the BSA, which redefines primary and secondary electronic evidence and mandates a dual-signature expert certificate (Section 63) for admissibility. Despite these legislative advancements, the research identifies systemic bottlenecks, including a 0% success rate in certain MLAT requests, critical shortages in forensic personnel, and a conviction rate of merely 886 cases against 86,420 registrations in 2023. The paper concludes that while the new laws represent a watershed moment, immediate investment in forensic infrastructure and "Examiners of Electronic Evidence" is required to prevent these statutes from remaining a "paper tiger".

KEYWORDS

Cyber Crime, Bharatiya Nyaya Sanhita (BNS), Electronic Evidence, Digital Forensics, Organized Crime, Data Protection.

I. INTRODUCTION

The Digital Metamorphosis of Indian Criminal Jurisprudence

The legal landscape of India is currently witnessing its most significant

transformation in over a century and a half. For decades, the governance of criminal justice was anchored in a triad of colonial-era legislations: the Indian Penal Code (IPC), 1860; the Code of Criminal Procedure (CrPC), 1973; and the Indian Evidence Act (IEA), 1872. While these laws provided a robust foundation, they were conceived in an analog era, ill-equipped to address the complexities of a hyper-connected society where over 86% of households now possess internet connectivity.[1] The proliferation of cyberspace as a primary domain of human interaction and consequently, criminal activity necessitated a paradigm shift from a legal framework that treated technology as an ancillary tool to one that recognizes the digital realm as a distinct theatre of legal action.

This transition culminated in late 2023 with the enactment of the *Bharatiya Nyaya Sanhita* (BNS), the *Bharatiya Nagarik Suraksha Sanhita* (BNSS), and the *Bharatiya Sakshya Adhiniyam* (BSA), which replaced the IPC, CrPC, and IEA respectively.[2] [3] These new laws, operative from July 1, 2024, represent not merely a renaming exercise but a structural integration of technology into the DNA of the justice system. The legislative intent is clear: to modernize the penal code, streamline procedural justice through electronic means, and overhaul the evidentiary standards for digital records.[4] [5]

The urgency of this reform is underscored by the precipitous rise in cybercrime. According to the National Crime Records Bureau (NCRB) "Crime in India 2023" report, cybercrime incidents have surged by 217% between 2018 and 2023.[6] In 2023 alone, 86,420 cases were registered, marking a significant increase from the previous year, with a crime rate rising to 6.2 per lakh population.[7] The financial ramifications are equally staggering, with losses attributed to cyber fraud estimated at ₹22,845 crore in 2024.[8] Against this backdrop, this research paper provides an

[1] PIB Delhi, 'India's Cyberspace Busy with Crores of Transactions' (Press Information Bureau, 6 January 2025) https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3 accessed 4 February 2026.
[2] *The Bharatiya Nyaya Sanhita 2023* (BNS).
[3] T*he Bharatiya Nagarik Suraksha Sanhita 2023* (BNSS).
[4] *The Bharatiya Sakshya Adhiniyam 2023* (BSA).
[5] Mayank Khichar, 'The Evolving Enigma: Electronic Evidence under the Bharatiya Sakshya Adhiniyam' (Vidhi Centre for Legal Policy, 1 October 2024) https://vidhilegalpolicy.in/blog/the-evolving-enigma/ accessed 4 February 2026.
[6] National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs 2024).
[7] 'NCRB's Crime in India 2023 Report' (Narayana IAS Academy, 30 September 2025) https://navigator.narayanaiasacademy.com/current-affairs/2025-09-30/ncrbs-crime-in-india-2023-report accessed 4 February 2026.
[8] 'India's cyber fraud epidemic: Rs 22,845 crore lost in 2024' *The Times of India* (New Delhi, 2024) https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms accessed 4 February 2026.

exhaustive analysis of the new legal framework governing cybercrimes in India, the procedural challenges inherent in digital investigations, and the evolving jurisprudence surrounding electronic evidence.

II. THE SUBSTANTIVE LEGAL FRAMEWORK: BHARATIYA NYAYA SANHITA (BNS), 2023

The *Bharatiya Nyaya Sanhita* (BNS), 2023, serves as the principal substantive criminal code. While it retains the core structure of the IPC, it introduces specific provisions that directly address the changing nature of criminality in the digital age. A critical analysis reveals that the BNS moves away from viewing cybercrimes solely through the prism of the Information Technology (IT) Act, 2000, integrating them instead into the general penal code to reflect their ubiquity.[9]

A. Organized Crime and the Cyber Syndicate (Section 111)

Perhaps the most potent addition to the BNS is Section 111, which introduces "Organized Crime" as a distinct offense. This section is a direct response to the industrialization of cyber fraud, often perpetrated by "fraud factories" and syndicates operating across jurisdictions.[10]

1. Defining the Offense

Section 111(1) defines organized crime as any "continuing unlawful activity" including, *inter alia*, economic offenses and "cyber-crimes having severe consequences," carried out by individuals acting singly or jointly as members of an organized crime syndicate.[11] This inclusion is pivotal. Previously, large-scale phishing operations or crypto-scams were prosecuted as individual acts of cheating (Section 420 IPC) or impersonation (Section 66D IT Act). Section 111 elevates these acts to organized crime when committed by a syndicate, acknowledging the structural nature of the threat.[12]

2. The Economic Offense Prism

The explanation to Section 111 broadens the scope of "economic offenses" to include:

---

[9] 'How BNS Addresses Cybercrimes: A Case Study' (LegalBlur, 2023) https://legalblur.com/how-bns-addresses-cybercrimes-a-case-study/ accessed 4 February 2026.

[10] BNS, s 111.

[11] 'Organised Crime under BNS' (Testbook, 2024) https://testbook.com/judiciary-notes/section-111-bns accessed 4 February 2026.

[12] 'Key Provisions Related to Cyber Crimes under BNS' (LawSection) https://lawsection.in/key-provisions-related-to-cyber-crimes-under-bharatiya-nyaya-sanhita-2023-bns-formerly-indian-penal-code-1860/ accessed 4 February 2026.

- **Mass-marketing fraud:** Targeted at phishing and lottery scams.
- **Ponzi schemes:** Often executed via cryptocurrency platforms.
- **Multi-level marketing schemes:** With the intent to defraud.
- **Money laundering and Hawala transactions:** Facilitated by digital wallets and dark web exchanges.[13]

The penalties are severe. If the offense results in the death of any person (a provision seemingly aimed at violent organized crime but legally applicable to cyber-extortion leading to suicide), the punishment is death or life imprisonment. In other cases, the minimum sentence is five years, extending to life. Furthermore, Section 111(3) criminalizes the abetment or facilitation of such crime, and Section 111(4) penalizes the harboring of syndicate members.

3. The Retrospectivity Controversy

A contentious aspect of Section 111 is the "continuing unlawful activity" clause, which requires that an activity is cognizable and punishable with imprisonment of three years or more, and that more than one charge-sheet has been filed before a competent court within the *preceding period of ten years*. Legal scholars argue this introduces a *de facto* retrospective application of the law. Investigating agencies can theoretically rely on charge-sheets filed under the old IPC (up to a decade ago) to establish the existence of a syndicate today, thereby invoking the harsher penalties of the BNS. This raises constitutional questions under Article 20(1) regarding *ex post facto* laws, although courts have generally interpreted "continuing offenses" as distinct from completed past acts.[14]

B. Cyber Fraud, Forgery, and Digital Deception

The BNS re-codifies traditional property offenses to explicitly include digital assets and electronic records, resolving ambiguities that plagued the IPC.

- **Cheating and Dishonest Inducement (Section 318):** Replaces Section 420 of the IPC. Section 318(4) is now the standard charge for "Cyber Fraud," covering acts of deception via digital means

[13] 'Key Provisions Related to Cyber Crimes under BNS' (LawSection) https://lawsection.in/key-provisions-related-to-cyber-crimes-under-bharatiya-nyaya-sanhita-2023-bns-formerly-indian-penal-code-1860/ accessed 4 February 2026.
[14] 'Double Jeopardy in India's Fight Against Organized and Financial Crime' (NUJS SACJ, 2024) https://www.nujssacj.com/post/double-jeopardy-in-india-s-fight-against-organized-and-financial-crime-section-111-bns-and-pmla accessed 4 February 2026.

that induce the delivery of property (including digital funds). The BNS definition of "property" and "valuable security" aligns with the digital reality, ensuring that theft of virtual assets falls within its ambit.[15]

- **Forgery of Electronic Records (Section 336):** Replaces the IPC's forgery provisions (Sections 463/464). Section 336 explicitly criminalizes the creation of false electronic records for the purpose of cheating or harming reputation. This is critical for prosecuting identity theft, deepfake creation (where used for fraud), and the manipulation of financial logs.

- **Identity-Based Offenses:** The BNS treats impersonation (Section 319(2)) with increased severity when used for cheating. In the context of "Digital Arrest" scams where perpetrators impersonate police officers via video calls police are invoking Sections 318(4) (Cheating) and 319(2) (Impersonation) of the BNS alongside IT Act provisions.

C. Offenses Against the State and Digital Sovereignty

The repeal of the sedition law (Section 124A IPC) was a headline reform of the BNS. However, it has been replaced by Section 152, which penalizes acts endangering the sovereignty, unity, and integrity of India. Crucially, Section 152 explicitly includes acts committed using "electronic communication" or "financial means".[16]

This provision creates a new category of "Digital Sovereignty" offenses. It targets:

1. **Cyber-terrorism:** Acts threatening economic security or striking terror (also covered under the UAPA).

2. **Disinformation Campaigns:** The use of electronic means to excite secession or armed rebellion.

Civil liberties organizations, such as the Internet Freedom Foundation (IFF), have critiqued the vagueness of terms like "subversive activities," arguing that Section 152 could potentially criminalize online dissent more broadly than the sedition law it replaced. The overlap with Section 66F of the IT Act (Cyber Terrorism) also creates a dual-charging scenario, allowing law enforcement to choose between the BNS and the IT Act

[15] BNS, ss 318, 336, 152, 75, 77, 78.

[16] Freedom House, 'Freedom on the Net 2024: India' (2024) https://freedomhouse.org/country/india/freedom-net/2024 accessed 4 February 2026.

based on procedural convenience.

D. Gender-Based Cyber Crimes

The BNS strengthens protections against online harassment, incorporating jurisprudence from landmark cases.

- **Voyeurism and Privacy (Section 77):** Criminalizes watching or capturing images of a woman engaging in a private act.
- **Stalking (Section 78):** Explicitly includes "cyberstalking" monitoring the use by a woman of the internet, email, or any other form of electronic communication.
- **Obscenity (Section 75):** Replaces Section 292 IPC, penalizing the sale or distribution of obscene material in electronic form. This must be read in consonance with *Shreya Singhal v. Union of India*, which narrowed the definition of online obscenity to protect free speech, ensuring the BNS is not used to censor legitimate expression.[17]

III. THE PROCEDURAL FRAMEWORK: BHARATIYA NAGARIK SURAKSHA SANHITA (BNSS), 2023

The *Bharatiya Nagarik Suraksha Sanhita* (BNSS), 2023, revolutionizes the procedural aspects of cyber investigation. Recognizing the volatility of digital evidence and the potential for tampering, the BNSS mandates the integration of technology into the investigative process itself.

A. Mandatory Audio-Video Recording of Search and Seizure

A historic shift in the BNSS is the mandatory requirement for videography during search and seizure operations, codified in Section 105.[18]

1. The Legal Mandate (Section 105)

Section 105 stipulates that the process of conducting a search of a place or taking possession of any property, article, or thing *shall* be recorded through audio-video electronic means, preferably a mobile phone. This recording must encompass:

- The entry into the premises.

[17] *Shreya Singhal v Union of India* (2015) 5 SCC 1.
[18] 'Recording of Search and Seizure: Electronic Mode' (LiveLaw, 2024) https://www.livelaw.in/articles/recording-of-search-and-seizure-electronic-mode-section-105-bnss-281366 accessed 4 February 2026.

- The discovery of the digital device.
- The preparation of the seizure list.
- The signing of the list by witnesses.

The recorded footage must be forwarded "without delay" to the District Magistrate, Sub-Divisional Magistrate, or Judicial Magistrate of the First Class. This provision aims to curb the rampant allegations of police planting evidence in cyber cases.[19]

2. Standard Operating Procedures (SOPs)

To implement this, the Bureau of Police Research and Development (BPR&D) has issued detailed SOPs. Key operational guidelines include:

- **Storage Media:** Recordings should be stored on a removable memory card, not the internal memory of the recording device, to ensure the card can be seized and sealed as evidence.
- **Chain of Custody:** The hash value of the video file must be generated immediately and mentioned in the seizure memo to ensure integrity.
- **Prohibition on Editing:** The video must not be viewed or edited on a computer prior to submission; any such interaction alters the metadata, rendering the evidence vulnerable to challenge under the BSA.

B. Forensic Examination and Crime Scene Management

Section 176(3) of the BNSS mandates that for any offense punishable with imprisonment of seven years or more, the officer in charge *shall* cause a forensic expert to visit the crime scene to collect forensic evidence. In the context of cybercrimes (e.g., Organized Cyber Crime under Sec 111 BNS), this makes the presence of a digital forensic analyst mandatory at the scene of the raid.

The Infrastructure Gap: While the law mandates forensic intervention, the infrastructure lags significantly. As of 2024, there are only 7 Central Forensic Science Laboratories (CFSLs) and roughly 24 State FSLs with digital forensic capabilities. With cybercrime cases exceeding 86,000 annually, the mandatory forensic visit clause (Sec 176(3)) threatens to create a massive bottleneck, potentially delaying investigations as police

[19] Bharat Chugh, 'BNSS: Mandatory Videography of Search & Seizure' (1 October 2024) https://bharatchugh.in/2024/10/01/bnss-mandatory-videography-of-search-seizure-a-few-thoughts/ accessed 4 February 2026.

await the availability of scarce experts.

C. Police Custody and Digital Decryption

Section 187 of the BNSS alters the police custody regime. Unlike the CrPC, which restricted police custody to the first 15 days post-arrest, the BNSS allows the 15-day custody period to be spread over the initial 40 or 60 days of judicial detention. **Implication for Cyber Investigations:** This is strategically vital for cybercrime. Decrypting a seized device, accessing cloud backups, or awaiting a response from a foreign service provider (e.g., Google or Meta) often takes weeks. The flexible custody provision allows police to return an accused to judicial custody while technical analysis proceeds, and seek police custody again *after* incriminating data is recovered, to confront the accused with new evidence.[20]

D. Digital Asset Seizure (Section 107)

Section 107 of the BNSS restructures the power to seize property, specifically acknowledging "digital and electronic assets". This empowers investigating officers to freeze cryptocurrency wallets and digital accounts suspected to hold proceeds of crime. However, unlike the PMLA, the BNSS lacks specific safeguards for the release of legitimate funds frozen during this process, raising concerns about potential misuse in freezing business accounts during investigations.

IV. THE EVIDENTIARY FRAMEWORK: BHARATIYA SAKSHYA ADHINIYAM (BSA), 2023

The admissibility of electronic evidence has been the most litigated aspect of Indian cyber law. The *Bharatiya Sakshya Adhiniyam* (BSA), 2023, attempts to settle the jurisprudential turbulence caused by conflicting Supreme Court judgments (*Anvar P.V.* vs. *Shafhi Mohammad* vs. *Arjun Panditrao*).[21]

A. "Primary" vs. "Secondary" Electronic Evidence

The BSA introduces a fundamental classification change. Under the IEA, electronic records were largely treated as secondary evidence requiring certification. The BSA, under Section 57, expands the definition of **Primary Evidence** to include certain electronic records.[22]

[20] BNSS, s 107.
[21] 'SOP 13-2025: Guidelines on Sequence of Custody' (Odisha Police CID CB 2025) https://odishapolicecidcb.gov.in/sites/default/files/SOP%2013-2025.pdf accessed 4 February 2026.
[22] BSA, s 57.

Provision	Nature of Evidence	Description
Section 57 Explanation 4	Primary	Electronic records stored in "semiconductor memory" (e.g., SD cards, internal phone storage) produced for the inspection of the Court.
Section 57 Explanation 5	Primary	Video recordings stored in electronic form and transmitted or broadcast.
Section 57 Explanation 6	Primary	Video recordings produced for the inspection of the Court.

This implies that if a smartphone containing an incriminating video is physically produced in court, it may be treated as primary evidence, theoretically bypassing the need for a certificate. However, this interpretation is fraught with technical risk, as accessing the "primary" device in court can alter its hash value and metadata.

B. The New Admissibility Regime: Section 63

Section 63 of the BSA replaces the erstwhile Section 65B of the IEA. While Section 61 declares that the admissibility of an electronic record cannot be denied *solely* on the ground that it is electronic, Section 63 lays down the mandatory conditions for its admission.[23]

1. The Expert Certificate (Section 63(4))

The most controversial provision is Section 63(4), which mandates a certificate for the admissibility of electronic records. Unlike the IEA, which required a certificate from a "person occupying a responsible official position," Section 63(4) of the BSA requires the certificate to be signed by two entities:

1. The person in charge of the computer/device.
2. An Expert

2. The "Expert" Definition Crisis

The BSA does not explicitly define who this "expert" is within the section. However, Section 39(2) implies that an "Examiner of Electronic Evidence"

[23] BSA, s 63(4).

notified under Section 79A of the IT Act is deemed an expert. **The Practical Bottleneck:** This dual-signature requirement creates a logistical nightmare. Requiring a Section 79A expert (typically found only in Central/State FSLs) to certify every piece of electronic evidence from a simple email printout to a complex server log imposes an impossible burden on the forensic infrastructure.

- *Legal Opinion:* Critics argue that this requirement, while intended to ensure authenticity, may lead to the exclusion of genuine evidence simply due to the unavailability of an expert signature, or conversely, reduce the "expert" signature to a bureaucratic rubber stamp.

3. Hash Values and Chain of Custody

The BSA Schedule and the BPR&D SOPs emphasize the role of **Hash Values** (digital fingerprints like MD5 or SHA-256). The certificate under Section 63(4) must explicitly mention the hash value of the evidence.

- **Procedure:** When a device is seized, its hash value must be computed at the scene (or immediately at the lab) and recorded.
- **Admissibility:** Any discrepancy between the hash value in the certificate and the hash value of the file produced in court indicates tampering, rendering the evidence inadmissible.

C. Judicial Interpretation: The Post-BSA Era

The courts are already grappling with these provisions. In *Vishnu Mohan v. State of Kerala* (July 2025), the Kerala High Court applied the BNS and BSA in a cyber-harassment case. The court's approach suggests a strict adherence to the procedural safeguards of the BNSS (video recording) while balancing the bail rights of the accused. Meanwhile, the "certificate" debate continues. While the Supreme Court in *Arjun Panditrao* settled that the 65B certificate was mandatory, the new *Alukas Jewelerry v. Anil* (2025) decision by the Kerala High Court suggests that the absence of a certificate might be a "curable defect," a view that conflicts with the strict text of Section 63(4) BSA. This judicial oscillation creates uncertainty for investigators and defense counsels alike.

V. THE INFORMATION TECHNOLOGY ACT, 2000: THE SPECIAL STATUTE

While the BNS provides the general penal framework, the Information Technology (IT) Act, 2000 remains the *lex specialis* for technical cybercrimes.

A. Intermediary Liability (Section 79) and the 2025 Amendments

Section 79 of the IT Act provides "safe harbor" to intermediaries (social media platforms, ISPs), protecting them from liability for third-party content provided they observe "due diligence." **The Shift to Active Policing:** The *IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, significantly diluted this safe harbor. The **2025 Amendments** to these rules have further tightened the noose.

- **Authorized Officers:** The 2025 rules specify the rank of officers authorized to issue takedown notices, bringing clarity but also increasing state control.
- **Proactive Monitoring:** Platforms are now arguably required to be "proactive arbiters" of content, especially regarding deepfakes and synthetic media, moving away from the "passive conduit" model established in *Shreya Singhal*.
- **Constitutionality:** The Karnataka High Court in *X Corp v. Union of India* (2024-25) upheld the government's power to issue blocking orders, reinforcing the state's grip on the digital narrative.

B. Data Protection and Law Enforcement Exemptions

The *Digital Personal Data Protection (DPDP) Act, 2023*, significantly impacts cyber investigations.

- **Section 17 Exemptions:** The Act exempts the processing of personal data for the "prevention, detection, investigation" of offenses from the requirement of user consent.
- **Implication:** Police do not need a suspect's consent to access their data from a "Data Fiduciary" (e.g., a telecom company or bank). However, the principles of necessity and proportionality, derived from the *Puttaswamy* judgment, still apply. The DPDP Act does not grant *carte blanche* for mass surveillance.

VI. INVESTIGATION CHALLENGES: THE REALITY ON THE GROUND

Despite the robust legal text, the enforcement of cyber laws in India faces systemic hurdles that often derail investigations.

A. The MLAT Crisis and Cross-Border Data

Cybercrime is borderless; Indian law enforcement is not. A vast majority of digital evidence (emails, social media logs) resides on servers in the United States. Accessing this data requires a Mutual Legal Assistance

Treaty (MLAT) request, a process plagued by extreme friction.

- **The "0%" Production Rate:** Transparency reports from 2024 indicate that for some platforms (e.g., WordPress), India had a **0% success rate** in obtaining information through MLATs, compared to 86% for US domestic requests.
- **Delays:** MLAT requests often take 10-24 months. In the fast-paced world of cybercrime, where logs are overwritten and IP addresses reassigned, this delay is often fatal to the investigation.
- **Encryption:** The "Going Dark" problem persists. End-to-end encryption on platforms like WhatsApp prevents law enforcement from accessing content even with a court order. While the IT Rules mandate "originator tracing," technical implementation remains contested and easily circumvented by criminals using VPNs or foreign SIMs.

B. The Forensic Bottleneck

The gap between the legislative mandate (mandatory forensics under BNSS Sec 176) and institutional capacity is the single biggest failure point.

- **Personnel Shortage:** FSLs are severely understaffed. The waiting period for a DNA or Cyber Forensic report can stretch to years.
- **Equipment Deficit:** Many state FSLs lack the advanced tools required to crack modern encryption or analyze proprietary file systems found in Apple devices or high-end crypto-wallets.
- **Expert Availability:** The requirement for an expert to physically visit crime scenes (Sec 176(3) BNSS) and sign evidence certificates (Sec 63 BSA) is physically impossible given the current ratio of experts to crimes.

C. The "Digital Arrest" Phenomenon

A specific challenge in 2024-25 has been the "Digital Arrest" scam. Criminals use high-quality video setups to impersonate judges or CBI officers, "arresting" victims digitally and forcing them to transfer funds to "verify" their innocence. **Jurisdictional Complexity:** These scams often involve VOIP calls from Southeast Asia, money mules in different Indian states, and crypto-offramps in Dubai. Coordinating an investigation across these multiple jurisdictions under the BNSS requires a level of inter-agency cooperation that is currently lacking.

VII. SOCIO-LEGAL STATISTICS: THE NCRB 2023 ANALYSIS

The NCRB 2023 data provides a quantitative dimension to the legal analysis.

- **Volume:** 86,420 cases registered (2023), a 31.1% increase year-on-year.
- **Motive:** Fraud dominates the landscape, accounting for 68.9% (59,526 cases) of all cybercrimes. This validates the BNS focus on "economic offenses" in Section 111.
- **Vulnerability:** Sexual exploitation accounts for 4.9% of cases, highlighting the continuing gendered dimension of cyber violence.
- **Regional Disparity:** Karnataka (Bengaluru) leads with 21,889 cases, reflecting the correlation between high tech adoption and cyber vulnerability. Conversely, Delhi reported only 407 cases in the "Northern Region" subset (likely under-reported or categorized differently), while Punjab saw a decline.
- **Conviction Rate:** Only 886 cases resulted in conviction in 2023. This abysmally low number reflects the investigation challenges (MLATs, forensics) and the difficulty of proving electronic evidence in court.

Statistic Category	**Data Point (2023)**	**Insight**
Total Cases	86,420	3x rise since 2018 (27,248 cases)
Cybercrime Rate	6.2 per lakh	Increasing digital penetration risk
Major Motive	Fraud (68.9%)	Validates Sec 111 BNS Economic Offense focus
Convictions	886	Severe gap in prosecutorial success

VIII. CONCLUSION AND RECOMMENDATIONS

The enactment of the BNS, BNSS, and BSA marks a watershed moment in India's fight against cybercrime. By defining organized cybercrime (Sec 111 BNS), mandating procedural transparency (Sec 105 BNSS), and modernizing evidence rules (Sec 63 BSA), the state has signalled its intent to impose the rule of law on the digital wild west.

However, a chasm remains between the *law in books* and the *law in action*.

The mandatory forensic provisions are threatened by infrastructural deficits; the cross-border data access regime is broken; and the "expert" certification requirement risks clogging the judicial machinery.

Recommendations:

1. **Forensic Capacity Building:** An immediate, massive investment in FSL infrastructure and the recruitment of "Examiners of Electronic Evidence" (Sec 79A IT Act) is non-negotiable to meet the mandates of BNSS and BSA.

2. **MLAT Reform:** India must aggressively pursue the "CLOUD Act" executive agreement with the US or finalize its accession to the Budapest Convention to streamline cross-border data access.

3. **Clarifying the "Expert":** The Ministry of Home Affairs must issue a notification clearly defining "Expert" under Section 63(4) BSA to include a broader range of qualified professionals, not just Section 79A government examiners, to prevent a judicial bottleneck.

4. **Harmonization:** Guidelines should be issued to prevent the "double jeopardy" of charging accused under both the BNS (Organized Crime) and PMLA for the same financial cyber acts.

While the legal framework is now robust and forward-looking, its success depends entirely on the capacity of the Indian state to implement the technological and procedural mandates it has set for itself. Without this, the new laws risk remaining a "paper tiger" in the face of an increasingly sophisticated digital adversary.

BIBLIOGRAPHY

I. Primary Legislative Sources (Statutes and Acts)

- **The New Criminal Laws (2023):**
    - *Bharatiya Nyaya Sanhita* (BNS), 2023.
    - *Bharatiya Nagarik Suraksha Sanhita* (BNSS), 2023.
    - *Bharatiya Sakshya Adhiniyam* (BSA), 2023.
- **Special Statutes:**
    - *The Information Technology Act, 2000* (including the *IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* and *2025 Amendments*),.

- *The Digital Personal Data Protection (DPDP) Act, 2023*.
- *Prevention of Money Laundering Act* (PMLA).
- *Unlawful Activities (Prevention) Act* (UAPA).

- **Repealed/Reference Legislations:**
  - *Indian Penal Code* (IPC), 1860.
  - *Code of Criminal Procedure* (CrPC), 1973.
  - *Indian Evidence Act* (IEA), 1872.

II. Judicial Precedents (Case Law)

- **Supreme Court of India:**
  - *Shreya Singhal v. Union of India* (Regarding online obscenity and intermediary liability),.
  - *Justice K.S. Puttaswamy (Retd.) v. Union of India* (Referred to as *Puttaswamy*; regarding privacy, necessity, and proportionality).
  - *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (Referred to as *Arjun Panditrao*; regarding Section 65B certificates).
  - *Anvar P.V. v. P.K. Basheer* (Referred to as *Anvar P.V.*).
  - *Shafhi Mohammad v. State of Himachal Pradesh* (Referred to as *Shafhi Mohammad*).

- **High Courts:**
  - *Vishnu Mohan v. State of Kerala* (Kerala High Court, July 2025; regarding BNS and BSA application).
  - *Alukas Jewelerry v. Anil* (Kerala High Court, 2025; regarding the curability of certificate defects).
  - *X Corp v. Union of India* (Karnataka High Court, 2024-25; regarding government blocking orders).

III. Reports and Official Guidelines

- **Government Reports:**

- National Crime Records Bureau (NCRB), "*Crime in India 2023*" (Published by Ministry of Home Affairs),.

- **Standard Operating Procedures:**

  - Bureau of Police Research and Development (BPR&D), *SOPs on Mandatory Audio-Video Recording of Search and Seizure under Section 105 BNSS*.

  - Bureau of Police Research and Development (BPR&D), *SOPs on Hash Values and Chain of Custody*.

IV. Secondary Sources and Commentary

- **Organizations:**

  - Internet Freedom Foundation (IFF) (Critique on Section 152 BNS regarding "subversive activities").

- **Concepts and Definitions:**

  - "Digital Arrest" (Emerging crime trends involving Sections 318(4) and 319(2) BNS).

- "Digital Sovereignty" (Relating to Section 152 BNS).