INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBERCRIME INVESTIGATION UNDER THE BHARATIYA NYAYA SANHITA, 2023: EMERGING ISSUES AND SOLUTIONS

AUTHORED BY - TARUN VERMA

Abstract

The Bharatiya Nyaya Sanhita (BNS), 2023, which replaced the Indian Penal Code, 1860 with effect from 1 July 2024, represents the most significant overhaul of India's substantive criminal law in over a century. Although the BNS does not codify a standalone chapter on "cyber offences," it extends established categories of crime — cheating, theft, forgery, identity offences, sexual harassment, and organised crime — to acts "committed by electronic means," while its companion statutes, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 and the Bharatiya Sakshya Adhiniyam (BSA), 2023, introduce procedural and evidentiary mechanisms for digital investigation, including mandatory audio-video recording of search and seizure and revised rules on the admissibility of electronic records. This paper critically examines the architecture of cybercrime investigation under this new trifecta of criminal law, situates it against the pre-existing framework of the Information Technology Act, 2000, and analyses empirical trends in cybercrime registration and conviction drawn from National Crime Records Bureau (NCRB) data for 2018–2023. The study identifies a structural paradox at the heart of the reform: while cybercrime has grown over 200 per cent in five years and conviction rates remain below two per cent, the BNS continues to address cyber offences indirectly, through interpretive extension rather than dedicated codification. Emerging issues are examined under six heads — definitional ambiguity, overlapping jurisdiction between the BNS and the IT Act, cross-border attribution, capacity deficits in investigating agencies, chain-of-custody integrity for digital evidence, and the regulatory gap concerning artificial-intelligence-enabled offences such as deepfakes. The paper concludes with a set of doctrinal and institutional recommendations, including a dedicated cyber-offences chapter, harmonised definitions across the BNS, BNSS, BSA and IT Act, mandatory digital-forensics training benchmarks, and a unified cybercrime court infrastructure, aimed at translating the technological aspirations of the new criminal-law framework into investigative and prosecutorial outcomes.

ISSN: 2582-6433

Keywords: Bharatiya Nyaya Sanhita 2023; cybercrime investigation; Bharatiya Nagarik Suraksha Sanhita; digital evidence; Information Technology Act 2000; electronic record; cyber forensics; criminal law reform India

1. Introduction

India's criminal justice system underwent a foundational transformation on 1 July 2024, when three new statutes — the Bharatiya Nyaya Sanhita (BNS), 2023, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and the Bharatiya Sakshya Adhiniyam (BSA), 2023 — replaced the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973, and the Indian Evidence Act, 1872 respectively. The reform was framed by the government as an exercise in decolonisation and modernisation, with explicit reference to the integration of technology into criminal procedure and the recognition of offences "committed through electronic means." This rhetorical commitment arrives at a moment of acute strain: cybercrime in India rose from 27,248 registered cases in 2018 to 86,420 in 2023, an increase of over 200 per cent, even as conviction rates for such offences have remained below two per cent.

Cybercrime investigation occupies a peculiar position within this reform. Unlike sexual offences, organised crime, or terrorism — each of which received dedicated chapters or sections in the BNS — cybercrime has not been consolidated into a discrete offence category. Instead, the legislature chose to extend the vocabulary of existing offences (cheating, theft, forgery, criminal intimidation, voyeurism) to cover acts performed through computers, mobile devices, and electronic communication networks. This drafting choice has significant downstream consequences for investigation: agencies must read the BNS together with the BNSS for procedure, the BSA for evidentiary admissibility, and the Information Technology Act, 2000 for the small set of offences that remain exclusively cyber-specific, such as unauthorised access and the dissemination of obscene material in electronic form.

This paper undertakes a doctrinal and empirical examination of cybercrime investigation under this layered framework. It maps the relevant provisions of the BNS, BNSS, and BSA against pre-existing IT Act offences; analyses publicly available crime data to assess the practical performance of the investigative and prosecutorial machinery; and identifies the structural, technical, and institutional issues that continue to impede effective cybercrime investigation in India. The paper closes with concrete recommendations addressed to legislators, investigating agencies, and the judiciary.

ISSN: 2582-6433

2. Background: From the IPC and the IT Act to the BNS Era

Prior to 1 July 2024, cybercrime in India was governed by a dual-track system. The Information Technology Act, 2000 (as amended in 2008) created a specialised regime of cyber offences — unauthorised access and data theft (Section 43/66), identity theft (Section 66C), cheating by personation using a computer resource (Section 66D), violation of privacy (Section 66E), cyber terrorism (Section 66F), and publication of obscene or sexually explicit material (Sections 67, 67A, 67B) — alongside special investigative powers for police officers under Sections 78 and 80. Simultaneously, the Indian Penal Code, 1860 continued to apply to cyber-enabled versions of traditional offences such as cheating (Section 420 IPC), criminal breach of trust, forgery, and defamation, since courts had consistently held that the medium of commission (electronic versus physical) did not alter the essential character of these offences.

This dual-track arrangement produced persistent overlap and forum confusion. Investigating officers frequently registered First Information Reports under both the IPC and the IT Act for a single transaction — for instance, an online financial fraud might attract Section 420 IPC for cheating and Section 66D of the IT Act for cheating by personation using a computer resource. Legal commentary prior to the 2023 reform repeatedly flagged the absence of a unified definition of "cybercrime" and the resulting inconsistency in charge-sheeting practices across States.

The Bharatiya Nyaya Sanhita, 2023 was drafted against this backdrop. According to PRS Legislative Research's analysis of the Bill, the BNS retains the great majority of IPC offences while adding twenty new offences, including organised crime and terrorism, and explicitly lists cybercrime committed on behalf of a crime syndicate as a form of organised crime. The Bharatiya Nagarik Suraksha Sanhita, 2023 simultaneously introduced provisions for the use of audio-video electronic means at multiple stages of investigation and trial, a forensic-evidence mandate for serious offences, and digitally enabled summons and search procedures. The Bharatiya Sakshya Adhiniyam, 2023 reworked the rules on documentary and electronic evidence inherited from Section 65B of the Indian Evidence Act, 1872, expanding the definition of "document" and "evidence" to expressly include electronic and digital records.

It is against this three-statute architecture, read alongside the surviving provisions of the IT Act, 2000, that the present-day framework for cybercrime investigation in India must be understood.

ISSN: 2582-6433

3. Research Objectives and Methodology

This paper pursues four objectives: (a) to map the substantive provisions of the BNS, 2023 that apply to cyber-enabled offences; (b) to examine the procedural and evidentiary innovations introduced by the BNSS and BSA, 2023 for digital investigation; (c) to assess, through secondary empirical data, the practical performance of the cybercrime investigation and prosecution machinery; and (d) to identify emerging legal and institutional issues and propose reform measures.

The study adopts a doctrinal-cum-empirical methodology. The doctrinal component involves textual and comparative analysis of the BNS, 2023, BNSS, 2023, BSA, 2023, and the Information Technology Act, 2000, supplemented by secondary legal commentary from law firms, academic journals, and parliamentary research bodies. The empirical component draws on publicly available National Crime Records Bureau (NCRB) data, Lok Sabha replies, and government press releases on cybercrime registration, charge-sheeting, and conviction for the period 2018–2023 — the most recent period for which consolidated cybercrime statistics are publicly available at the time of writing. Because the NCRB's "Crime in India 2023" report is the last to be compiled wholly under the IPC-era classification (with future reports expected to migrate to BNS-based crime heads), the data presented here serves primarily as a baseline against which the effectiveness of the new framework can subsequently be measured. Figures presented in Section 7 should accordingly be read as indicative of underlying trends rather than as precise post-reform performance metrics.

Limitations of the study include the unavailability, as of mid-2026, of consolidated NCRB data specifically classified under BNS sections (since the transition occurred only in July 2024 and crime statistics are typically published with a lag of twelve to eighteen months), and the consequent reliance on illustrative or proxy figures for certain categorical breakdowns, which are flagged accordingly wherever used.

4. Substantive Framework: Cyber Offences under the BNS, 2023

The BNS, 2023 does not contain a chapter titled "cyber offences." Instead, cyber-enabled conduct is captured through three drafting techniques: first, the retention of technologically neutral offence definitions (such as cheating and forgery) that apply irrespective of medium; second, the explicit insertion of the phrase "electronic means" or "electronic communication"

ISSN: 2582-6433

into specific provisions, such as those governing voyeurism, stalking, and offences against the State; and third, the creation of a new aggravated offence — organised crime under Section 111 — that expressly names cybercrime as a predicate activity when committed by or on behalf of a crime syndicate.

4.1 Key Provisions and their Cyber Application

Table 1 summarises the principal BNS provisions relevant to cybercrime investigation, mapped against their predecessor IPC sections and their typical cyber application.

BNS, 2023 Section	Predecessor (IPC)	Offence	Typical Cyber Application
Section 111	New provision	Organised Crime	Cyber-enabled organised fraud, phishing syndicates, card-skimming and scam-call networks operated by crime syndicates
Sections 316–318	Ss. 405, 415, 420	Criminal Breach of Trust / Cheating	UPI and online banking fraud, fake investment and trading-app scams, OTP fraud
Section 319	Ss. 416, 419	Cheating by Personation	Fake social-media profiles, impersonation for fraud or harassment
Sections 303–306	Ss. 378–382	Theft	Unauthorised access to and removal of digital data / data theft (read with IT Act, S. 43)
Sections 336–340	Ss. 463–477A	Forgery / Forged Electronic Record	Tampering with electronic records, forged digital documents and signatures
Section 78	S. 354D	Stalking	Monitoring a person's use of the internet, email or electronic communication; cyberstalking
Section 77	S. 354C	Voyeurism	Non-consensual capture or dissemination of private images (“revenge porn”, NCII)
Sections 294–295	Ss. 292–294	Obscenity	Distribution of obscene material

ISSN: 2582-6433

			through electronic/digital platforms
Section 356	S. 499	Defamation	Online and social-media defamation
Sections 351–352	S. 503/506	Criminal Intimidation	Online threats, sextortion, blackmail via electronic communication
Section 152	Sedition (S. 124A, repealed)	Acts Endangering Sovereignty, Unity and Integrity of India	Online content threatening national security or public order
Section 197	S. 505	Statements Conducing to Public Mischief	Misinformation/false statements transmitted through electronic communication

Table 1: Mapping of BNS, 2023 Provisions Relevant to Cybercrime (compiled by author from BNS, 2023 and secondary legal commentary).

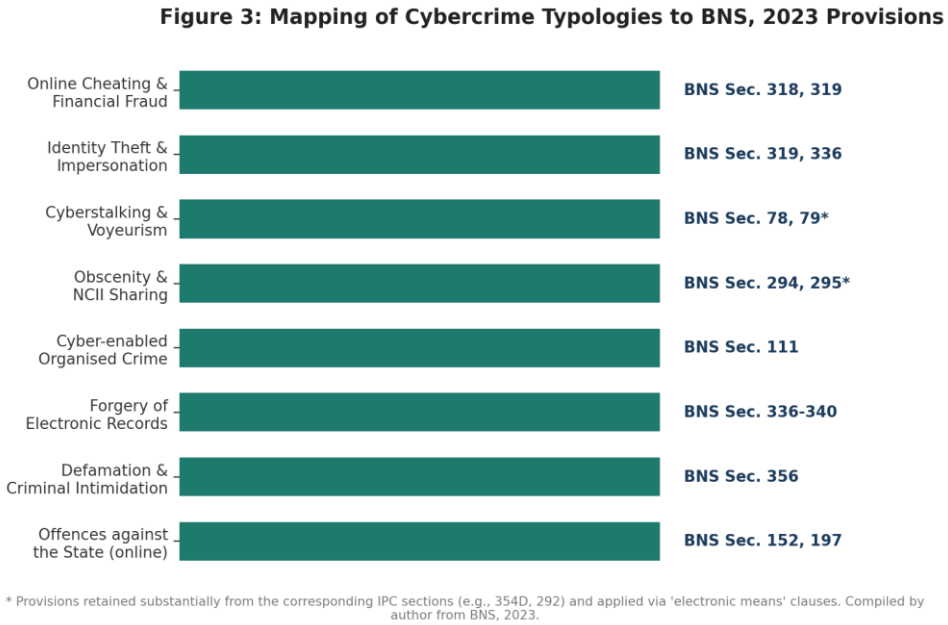


Figure 3: Mapping of cybercrime typologies to BNS, 2023 provisions, illustrating the dispersed rather than consolidated drafting approach.

4.2 The Organised Crime Provision and its Limits

Section 111 of the BNS is the only provision that names cybercrime in express terms, defining organised crime to include continuing unlawful activity such as kidnapping, extortion, contract

ISSN: 2582-6433

killing, land grabbing, economic offences, and cybercrime, undertaken by a crime syndicate, whether singly or jointly, for material or other benefit. Commentary on the provision, including analysis by the Esya Centre, has observed that the absence of a statutory definition of "cybercrime" within the BNS itself creates interpretive ambiguity: investigators and courts are left to determine, in each case, whether a given act of online fraud or hacking meets the threshold of organised, syndicate-level activity required to invoke Section 111, or whether it should instead be charged purely as cheating, theft, or an IT Act offence. The provision therefore functions as an aggravating mechanism for cyber-enabled organised crime rather than as a general cybercrime statute, leaving the bulk of individual cyber offences to be addressed through the ordinary, technologically neutral provisions listed in Table 1.

4.3 Offences against Property and Documents

The chapters on offences against property (Sections 303–334) and offences relating to documents (Sections 335–350) retain the structure of their IPC predecessors but are understood, consistent with prior judicial interpretation of the IPC, to extend to digital and electronic forms of property and documentation. Section 318, the principal cheating provision, has emerged in practice as the primary charge for online financial fraud, including UPI fraud, fake trading-application scams, and digital-arrest extortion schemes, because the offence is defined in terms of deception and wrongful gain or loss, irrespective of the medium of deception.

5. Investigative and Procedural Framework under the BNSS, 2023

If the BNS supplies the substantive offences, the Bharatiya Nagarik Suraksha Sanhita, 2023 supplies the procedural architecture for investigating them, and it is here that the most explicit recognition of digital investigation appears. The Statement of Objects and Reasons of the BNSS specifically refers to the use of technology and forensic science in criminal investigation, and several provisions operationalise this commitment.

5.1 Mandatory Audio-Video Recording of Search and Seizure

Section 105 of the BNSS is a new provision requiring that the process of searching a place or seizing property — including the preparation and signing of the seizure list — be recorded through audio-video electronic means, preferably by mobile phone, with the recording forwarded without delay to the jurisdictional Magistrate. A parallel requirement appears in Section 185 for search procedures generally, with a 48-hour transmission timeline to the

ISSN: 2582-6433

Magistrate empowered to take cognizance. For cybercrime investigation, this provision is directly relevant to the search and seizure of computers, servers, mobile devices, and storage media, since it creates a contemporaneous, tamper-evident record of how digital evidence was located, handled, and packaged — a safeguard aimed at strengthening the chain of custody that has historically been a point of vulnerability in digital-evidence cases.

5.2 Mandatory Forensic Examination for Serious Offences

Section 176(3) of the BNSS requires that, for offences punishable with seven years' imprisonment or more, a forensic expert visit the crime scene to collect forensic evidence, and, where Mobile Forensic Science Laboratories are unavailable, that the visit and process be assessed through technological means. Given that several cyber-enabled offences captured under the BNS (such as cheating, organised crime, and extortion involving digital means) are punishable with sentences crossing this threshold, the provision creates an indirect statutory expectation of digital and cyber-forensic involvement at the investigation stage, moving the system away from a purely confession- or testimony-driven model of evidence-gathering.

5.3 Technology-Enabled Trials and Proceedings

Section 530 of the BNSS contains a general enabling provision permitting trials, inquiries, and other proceedings to be conducted in electronic mode, including through audio-video electronic means. Courts, including a Division Bench of the Kerala High Court in Rollymol v. State of Kerala, have read this provision, together with Section 105, as reflecting a deliberate legislative emphasis on the use of modern technology at every stage of the criminal process, from investigation through trial.

5.4 Zero FIR, e-FIR, and Jurisdictional Flexibility

The BNSS statutorily embeds the “Zero FIR” mechanism — previously a judicial innovation traced to the Supreme Court's decision in Lalita Kumari v. Government of Uttar Pradesh — allowing a First Information Report to be registered at any police station irrespective of territorial jurisdiction, with subsequent transfer to the appropriate station. This is of particular significance for cybercrime, where the location of the victim, the perpetrator, the server, and the financial intermediary frequently differ, making strict territorial jurisdiction ill-suited to the nature of the offence. The framework operates alongside the National Cyber Crime Reporting Portal (cybercrime.gov.in), which allows victims to lodge complaints online, with serious matters subsequently requiring police-station-level follow-up.

ISSN: 2582-6433

5.5 Time-Bound Investigation and Trial

The BNSS introduces statutory timelines absent from the Code of Criminal Procedure, 1973, including a 60-day limit for framing of charges by a Sessions Court from the first hearing, and a 30-day (extendable to 45-day) limit for pronouncement of judgment after conclusion of arguments. While not cyber-specific, these timelines bear on cybercrime adjudication insofar as digital-evidence-heavy trials have historically suffered from prolonged delays linked to forensic backlogs and the technical complexity of presenting electronic evidence.

6. The Evidentiary Interface: BSA, 2023 and the IT Act, 2000

6.1 Electronic Records under the BSA, 2023

The Bharatiya Sakshya Adhiniyam, 2023 replaces the Indian Evidence Act, 1872 and revises the treatment of electronic evidence inherited from the much-litigated Section 65B of the 1872 Act. The BSA expands the statutory definition of "document" and "evidence" to expressly encompass electronic and digital records, including emails, server logs, locational evidence, and information stored on semiconductor memory, communication devices, and similar media. Sections of the BSA dealing with expert opinion (broadly corresponding to the former Sections 45–47 of the Evidence Act) have also been adapted to address electronic and digital evidence, recognising the centrality of forensic and technical experts in establishing the authenticity, integrity, and provenance of digital material presented at trial.

In practical terms, the certification requirements that previously governed the admissibility of electronic records under Section 65B(4) of the Evidence Act — the subject of extensive Supreme Court jurisprudence, notably Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal — continue in substance under the BSA's electronic-evidence provisions, meaning that investigators must still obtain a compliant certificate identifying the device, the manner of production, and the conditions under which the electronic record was generated, in order for that record to be admissible without the underlying device being produced in court.

6.2 Continuing Role of the Information Technology Act, 2000

The IT Act, 2000 has not been repealed and continues to operate as the primary source of several offences that remain definitionally cyber-specific and outside the scope of the BNS, including unauthorised access and damage to computer systems (Section 43, civil; Section 66, penal), identity theft (Section 66C), cheating by personation using a computer resource (Section 66D), violation of privacy through capturing or publishing images of a private area

ISSN: 2582-6433

(Section 66E), cyber terrorism (Section 66F), and the publication or transmission of obscene (Section 67), sexually explicit (Section 67A), and child sexual abuse material (Section 67B) in electronic form. Investigative powers of entry, search, and arrest for IT Act offences continue to be governed principally by Sections 78 and 80 of that Act, while the Indian Computer Emergency Response Team (CERT-In), constituted under Section 70B, retains its mandate to coordinate response to computer security incidents and to support investigating agencies with technical assistance.

The result is a layered, rather than unified, legal regime: a single cyber-enabled fraud may simultaneously attract charges under the BNS (cheating, forgery, criminal breach of trust), the IT Act (cheating by personation, unauthorised access), and, where applicable, special legislation such as the Prevention of Money Laundering Act, 2002. Investigating officers must therefore navigate at least three statutory frameworks — BNS, BNSS/BSA, and the IT Act — in building a single cybercrime case file, with the BNSS's procedural provisions and the BSA's evidentiary provisions applying uniformly across BNS and IT Act charges in a given case.

6.3 Intermediary Liability and Safe Harbour

Section 79 of the IT Act, which provides conditional safe-harbour protection to online intermediaries (social-media platforms, internet service providers, e-commerce platforms) from liability for third-party content, remains a critical and unresolved point of friction for cybercrime investigation. Investigators frequently depend on intermediaries for subscriber data, IP logs, and content takedown, and the adequacy, timeliness, and cross-border enforceability of such cooperation — particularly where the intermediary is headquartered outside India — continues to be a significant practical bottleneck, a theme examined further in Section 8.

7. Empirical Trends in Cybercrime Registration and Adjudication

This section presents NCRB-derived data on cybercrime registration and adjudication for 2018–2023, the final period reported under the IPC-era classification, to establish the empirical baseline against which the BNS framework's effectiveness will need to be assessed in subsequent reporting cycles.

7.1 Growth in Registered Cases

As Figure 1 and Table 2 show, cybercrime cases registered with police rose from 27,248 in 2018 to 86,420 in 2023 — a cumulative increase of approximately 217 per cent over five years,

ISSN: 2582-6433

with the steepest single-year rise (31.2 per cent) recorded between 2022 and 2023. According to the NCRB's "Crime in India 2023" report, this spike was driven principally by cheating through personation, with cybercrime registering the highest percentage increase of any major crime head that year, ahead of crimes against children, Scheduled Tribes, or property offences generally.

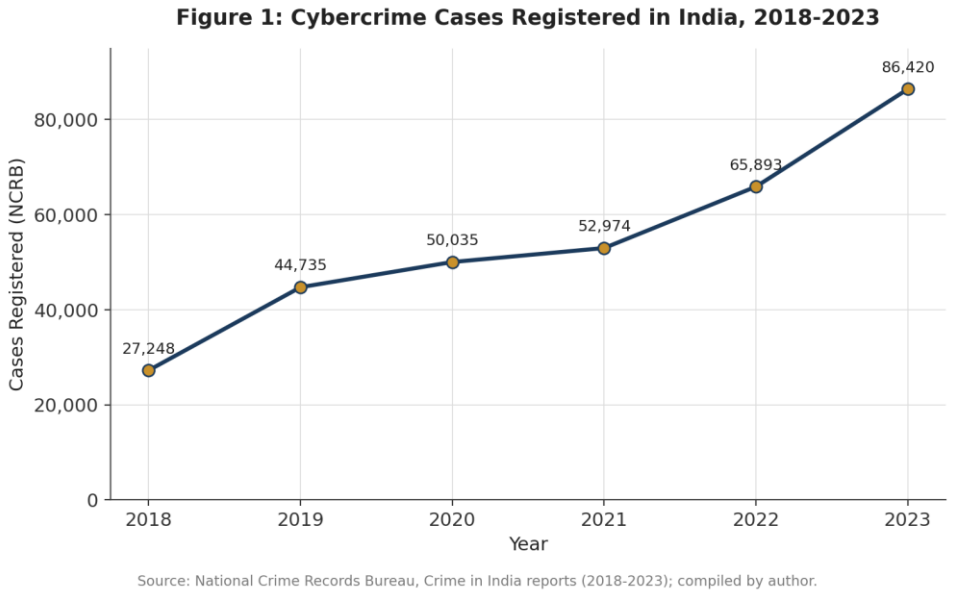


Figure 1: Cybercrime cases registered in India, 2018–2023 (Source: NCRB, Crime in India reports).

Year	Cases Registered	Year-on-Year Change	Notable Driver
2018	27,248	—	Baseline year
2019	44,735	+64.2%	Growth in online fraud reporting
2020	50,035	+11.8%	COVID-19 digital migration
2021	52,974	+5.9%	Continued digital-payments expansion
2022	65,893	+24.4%	UPI fraud, sextortion cases
2023	86,420	+31.2%	Cheating by personation; investment/trading-app scams

Table 2: Year-on-year growth in cybercrime registration, 2018–2023 (compiled by author from NCRB data and media reporting).

7.2 The Conviction Gap

Despite rising registration, conviction outcomes have not kept pace. Reporting based on NCRB data placed before Parliament indicates that, of approximately 1.67 lakh cybercrime cases

 ISSN: 2582-6433

registered across States between 2020 and 2022, only around 2,706 persons — roughly 1.6 per cent — were convicted. State-level figures show wide variance: Uttar Pradesh recorded comparatively higher conviction numbers (642 persons convicted out of 11,000 cases registered in 2020), while States such as Karnataka and Telangana, despite registering among the highest case volumes nationally, recorded conviction rates close to zero in several years.

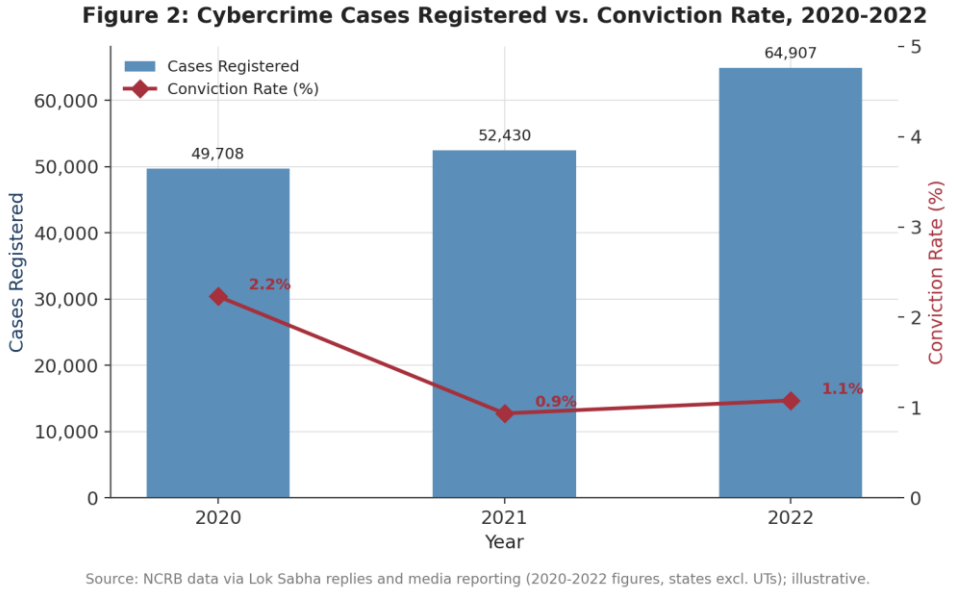


Figure 2: Cybercrime cases registered versus conviction rate, 2020–2022 (illustrative; Source: NCRB data via Lok Sabha replies and press reporting).

This persistent conviction gap is a central empirical justification for the present study: it indicates that the principal bottleneck in Indian cybercrime enforcement has historically lain less in the absence of applicable substantive offences — cheating and forgery provisions under the IPC were generally adequate to charge cyber fraud — and more in investigative capacity, digital-evidence handling, cross-border attribution, and prosecutorial follow-through. This has direct implications for how the procedural innovations of the BNSS and BSA, discussed in Sections 5 and 6, should be evaluated: their success will depend on implementation and capacity-building at least as much as on statutory design.

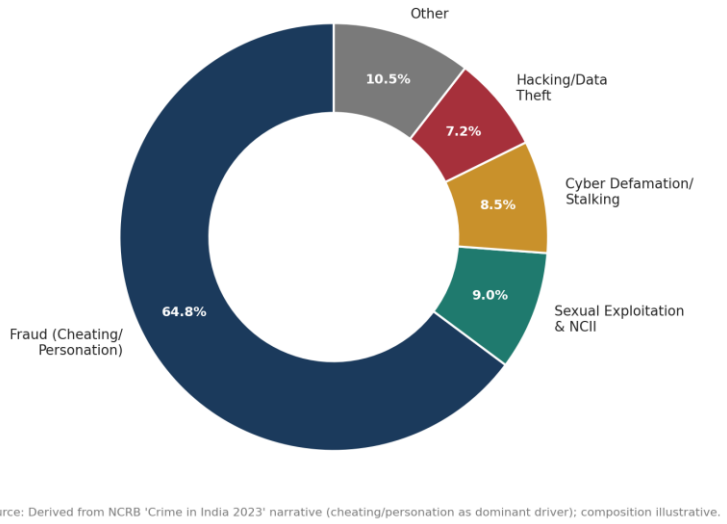
7.3 Composition of Cybercrime by Category

Consistent with the NCRB's identification of cheating through personation as the dominant driver of the 2023 spike, the broad composition of registered cybercrime continues to be weighted heavily towards financially motivated fraud, with sexual exploitation, defamation/stalking, and direct hacking/data-theft offences forming smaller but persistent shares. Figure 4 presents an illustrative breakdown of this composition, with cybercrimes

ISSN: 2582-6433

against women alone rising from 6,030 cases in 2018 to over 19,000 in 2023 — a more than threefold increase that signals the growing relevance of the BNS provisions on voyeurism, stalking, and criminal intimidation discussed in Section 4.

Figure 4: Illustrative Composition of Cybercrime Categories Registered in India, 2023



Source: Derived from NCRB 'Crime in India 2023' narrative (cheating/personation as dominant driver); composition illustrative.

Figure 4: Illustrative composition of cybercrime categories registered in India, 2023 (derived from NCRB narrative data; composition approximate).

8. Emerging Issues and Challenges

The transition to the BNS, BNSS, and BSA framework has not resolved — and in some respects has added new dimensions to — the structural challenges confronting cybercrime investigation in India. This section examines six principal issues.

8.1 Definitional Ambiguity and Fragmented Codification

As discussed in Section 4, the BNS uses the term “cybercrime” only once, in the organised-crime provision under Section 111, without defining it. Investigators consequently rely on charge-by-charge interpretation — deciding, for each act, whether it falls under cheating, theft, forgery, stalking, or organised crime — rather than applying a settled statutory taxonomy of cyber offences. Legal commentary, including analysis by the Esya Centre, has identified this absence of a clear definition as a source of ambiguity that affects charge-sheeting consistency and appellate interpretation. The dispersed drafting technique also makes it difficult to generate clean cybercrime-specific statistics under the new law, since BNS sections such as cheating or forgery capture both cyber and non-cyber instances of the same offence.

ISSN: 2582-6433

8.2 Overlapping and Parallel Proceedings

The continued, simultaneous operation of the BNS and the IT Act, 2000 means that a single transaction frequently generates overlapping charges — for example, cheating under the BNS and cheating by personation under Section 66D of the IT Act for the same act of online fraud. While such overlap is not new (it existed under the IPC/IT Act regime as well), the introduction of a new substantive code without a corresponding consolidation of the IT Act's offence provisions preserves, rather than resolves, the risk of forum-shopping, double jeopardy disputes, and inconsistent sentencing outcomes across the BNS and IT Act tracks for functionally identical conduct.

8.3 Cross-Border Attribution and Jurisdiction

NCRB and law-enforcement commentary increasingly highlight the cross-border character of Indian cybercrime, with a significant share of cases linked to operations based in Southeast Asian jurisdictions, including organised "scam compound" networks. The Zero FIR mechanism under the BNSS addresses domestic territorial jurisdiction but does not, by itself, resolve the more difficult problem of obtaining evidence, freezing assets, or securing arrest and extradition where the perpetrator, server infrastructure, or financial mule network is located outside India. India's reliance on Mutual Legal Assistance Treaties (MLATs) and bilateral law-enforcement cooperation remains comparatively slow relative to the speed at which digital fraud proceeds can be moved and laundered, and the BNS/BNSS framework does not introduce new fast-track international cooperation mechanisms specific to cybercrime.

8.4 Capacity, Training, and Forensic Infrastructure

Section 176(3) of the BNSS creates a statutory expectation of forensic involvement in serious offences, but India's forensic science laboratory (FSL) infrastructure has long been reported as understaffed and overburdened, with case backlogs extending investigation timelines well beyond the statutory limits the BNSS itself prescribes for charge-sheeting and trial. Cyber-forensic capability — the ability to image devices, recover deleted data, trace cryptocurrency transactions, and analyse server and application logs — requires specialised training that is unevenly distributed across States, with most dedicated cyber-forensic capacity concentrated in metropolitan cybercrime units. The conviction-rate disparities noted in Section 7.2, where higher-capacity States such as Uttar Pradesh recorded markedly better conviction outcomes than States with comparable or higher case volumes, are consistent with capacity, rather than purely legal, explanations for poor enforcement performance.

ISSN: 2582-6433

8.5 Chain of Custody and Evidentiary Integrity

While Section 105 of the BNSS introduces a valuable safeguard by mandating audio-video recording of search and seizure, the provision does not prescribe technical standards for such recording, storage, or subsequent verification, a gap noted in commentary on the section. For volatile digital evidence in particular — RAM contents, live network connections, cloud-stored data — the absence of detailed standard operating procedures creates a risk that evidence collected without adherence to internationally recognised digital-forensic protocols (such as write-blocking, hash verification, and documented custody logs) may be challenged on authenticity or integrity grounds at trial, notwithstanding compliance with the BSA's certification requirements for electronic records.

8.6 Artificial Intelligence, Deepfakes, and Regulatory Lag

Neither the BNS nor the IT Act, 2000 contains a provision specifically addressing AI-generated synthetic media ("deepfakes"), voice-cloning fraud, or algorithmically generated disinformation, despite the rapid emergence of these techniques as vectors for financial fraud (including impersonation of family members or executives in real-time voice/video calls), non-consensual intimate imagery, and election-related disinformation. Investigators are presently required to fit such conduct into existing categories — cheating, voyeurism, defamation, or obscenity — an approach that may prove adequate for outcome-based offences (where the harm, such as financial loss, is unaffected by whether the fraud was AI-assisted) but is more strained for conduct, such as the mere creation or circulation of a deepfake without an immediate quantifiable harm, that does not map cleanly onto pre-AI offence definitions.

8.7 Underreporting and Victim Access

Parliamentary responses from the Ministry of Home Affairs acknowledge that specific data on what proportion of online-fraud and cybercrime victims actually report the offence to authorities is not centrally compiled, suggesting that registered case figures — already showing steep growth — likely understate the true incidence of cybercrime. Barriers to reporting include limited awareness of the National Cyber Crime Reporting Portal, the perceived futility of reporting low-value financial fraud given the low conviction rates documented in Section 7.2, and the technical complexity victims face in articulating a complaint in a form usable for investigation.

ISSN: 2582-6433

9. Comparative Perspective

India's approach — extending general criminal-law provisions to cyber conduct while retaining a separate, narrower IT statute for genuinely cyber-specific offences — differs from jurisdictions that have adopted dedicated cybercrime codes. The United Kingdom's Computer Misuse Act, 1990 and the United States' Computer Fraud and Abuse Act, 1986 each consolidate unauthorised access and related computer offences within a single specialised statute, providing greater definitional clarity than India's current dispersed model, though both have separately faced criticism for failing to keep pace with cloud computing and cross-border data flows. The Council of Europe's Budapest Convention on Cybercrime (2001), to which India is not a signatory, establishes a harmonised framework for substantive offences, procedural powers, and — most significantly for the cross-border issues identified in Section 8.3 — expedited international cooperation and mutual legal assistance specific to cybercrime and electronic evidence. India's non-participation in the Budapest Convention, combined with its continued reliance on conventional MLAT channels, leaves a structural gap in fast-track cross-border evidence-sharing that the BNS/BNSS reforms, being domestically focused, do not address. Some scholars have suggested that India's preference for a sui generis, non-Budapest framework reflects sovereignty and data-localisation concerns, but the practical cost is borne by investigating agencies confronting foreign-hosted infrastructure and offshore scam operations.

10. Recommendations and the Way Forward

Drawing on the doctrinal mapping in Sections 4–6 and the empirical and institutional issues identified in Section 8, this paper proposes the following measures, summarised in Table 3.

1. Consolidate a definitional anchor for cybercrime. While full codification of a separate cybercrime chapter may not be necessary, the BNS should be amended to insert a working definition of “offence committed by electronic means,” which would apply uniformly across the cheating, theft, forgery, stalking, and organised-crime provisions identified in Table 1, reducing reliance on ad hoc judicial interpretation.
2. Harmonise the BNS and the IT Act through prosecutorial guidelines. Pending fuller legislative consolidation, the Ministry of Home Affairs and State police establishments should issue binding charge-sheeting guidelines clarifying when BNS provisions, IT Act provisions, or both should be invoked for a given category of cyber-enabled conduct, reducing inconsistency and duplicative litigation.

ISSN: 2582-6433

3. Operationalise Section 105 BNSS with technical standard operating procedures. The Directorate of Forensic Science Services, in coordination with State forensic laboratories, should issue detailed protocols for digital evidence handling during search and seizure — covering write-blocking, cryptographic hashing, volatile-memory capture, and recording-storage standards — to give practical effect to the chain-of-custody safeguard envisaged by the provision.
4. Invest in cyber-forensic capacity proportionate to the Section 176(3) BNSS mandate. State governments should be supported, including through central financial assistance schemes, to expand cyber-forensic staffing, equipment, and Mobile Forensic Science Unit deployment to meet the forensic-evidence threshold the BNSS now imposes for offences carrying seven years' imprisonment or more, many of which now include cyber-enabled fraud and organised crime.
5. Strengthen cross-border cooperation mechanisms. India should expand 24x7 cybercrime points of contact under existing international frameworks, pursue closer cooperation with jurisdictions implicated in scam-compound operations, and evaluate the costs and benefits of alignment with or accession to the Budapest Convention's procedural cooperation provisions, to reduce MLAT-related delays in cross-border evidence gathering.
6. Introduce a targeted provision for AI-generated synthetic media abuse. A focused amendment criminalising the malicious creation, circulation, or commercial exploitation of non-consensual deepfake content, distinct from but complementary to the existing voyeurism and obscenity provisions, would close the regulatory gap identified in Section 8.6 ahead of further escalation in AI-enabled fraud and image-based abuse.
7. Establish specialised cybercrime courts and prosecutorial cadres. Given the technical complexity of digital evidence, dedicated cybercrime courts and trained special public prosecutors — building on existing fast-track court models for other offence categories — would improve both adjudication speed (supporting the BNSS's statutory trial timelines) and conviction outcomes.
8. Improve public cybercrime statistics and victimisation data. The NCRB and the Indian Cyber Crime Coordination Centre (I4C) should publish disaggregated, BNS-section-wise cybercrime data alongside periodic victimisation surveys, enabling more precise post-reform evaluation than is presently possible using IPC-era classifications.

ISSN: 2582-6433

Issue	Recommendation	Responsible Stakeholder
Definitional ambiguity (8.1)	Insert a consolidated definition of "cyber offence" in the BNS or a dedicated chapter cross-referencing existing provisions	Ministry of Home Affairs / Parliament
Overlapping proceedings (8.2)	Issue binding prosecutorial guidelines on charge selection between BNS and IT Act provisions for the same transaction	Ministry of Home Affairs; State DGPs
Cross-border attribution (8.3)	Pursue accession to or alignment with the Budapest Convention framework; expand 24x7 cybercrime liaison points	Ministry of External Affairs; MHA
Capacity and training (8.4)	Mandate minimum cyber-forensic training benchmarks and FSL staffing ratios tied to BNSS Section 176(3) implementation	State Governments; BPR&D
Chain of custody (8.5)	Issue standard operating procedures for Section 105 BNSS recording, hashing, and digital chain-of-custody documentation	MHA; Directorate of Forensic Science Services
AI / deepfake gap (8.6)	Introduce a specific provision criminalising malicious synthetic-media creation and non-consensual deepfake circulation	Parliament (BNS amendment) / MeitY
Underreporting (8.7)	Strengthen and publicise the National Cyber Crime Reporting Portal; institute periodic victimisation surveys	Indian Cyber Crime Coordination Centre (I4C)

Table 3: Summary of recommendations mapped to identified issues and responsible stakeholders (compiled by author).

11. Conclusion

The Bharatiya Nyaya Sanhita, 2023, together with the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam, represents a genuine, if partial, modernisation of India's approach to cybercrime investigation. The introduction of mandatory audio-video recording of search and seizure, a forensic-evidence mandate for serious offences, statutory Zero FIR provisions, and an expanded definition of electronic evidence collectively signal a legislative intent to align criminal procedure with the realities of digital-era offending. At the same time,

ISSN: 2582-6433

the substantive treatment of cybercrime within the BNS remains fragmented: the absence of a consolidated definition or chapter, the continued, overlapping operation of the Information Technology Act, 2000, and the lack of any provision addressing AI-generated synthetic media indicate that the reform has not fully closed the gap between legislative ambition and investigative reality.

The empirical record reinforces this assessment. Cybercrime registration in India grew by over 200 per cent between 2018 and 2023, while conviction rates over the same period remained below two per cent — a gap that reflects deficits in forensic capacity, cross-border cooperation, and prosecutorial follow-through at least as much as deficiencies in the underlying substantive law. The success of the BNS/BNSS/BSA framework in addressing cybercrime will therefore depend less on the text of any single section than on the institutional capacity — forensic infrastructure, trained personnel, specialised courts, and international cooperation mechanisms — built to give effect to it. Future research, drawing on BNS-classified crime data as it becomes available from 2025 onward, will be needed to assess whether the structural reforms examined in this paper have begun to narrow the persistent gap between cybercrime incidence and successful prosecution in India.

References

Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), Ministry of Home Affairs, Government of India.

Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023), Ministry of Home Affairs, Government of India.

Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), Ministry of Home Affairs, Government of India.

Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008).

PRS Legislative Research. “The Bharatiya Nyaya Sanhita, 2023.” Bill Track summary, PRS India.

Esya Centre. “The New Criminal Laws and Their Interface with Technology.” Perspectives, 31 July 2024.

Lawctopus. “Decoding the BNSS 2023: Key Provisions, Changes & More.” 24 October 2025.

LiveLaw. “Recording of Search and Seizure through Audio-Video Electronic Means under Section 105 of the BNSS.” 19 January 2025.

ISSN: 2582-6433

Nishith Desai Associates. “Navigating Through Criminal Law Reforms: Part II — Review of the Bharatiya Nagarik Suraksha Sanhita, 2023.”

Bar and Bench. “Revolutionising Digital Forensics: India's New Legal Frontiers.” 27 July 2024.

The420.in. “The Role of Digital Forensics and Cyber Crime Provisions in India's New Criminal Laws.” 28 July 2024.

MCO Legals. “Cybercrimes under the Bhartiya Nyaya Sanhita, 2023.” Cyber Law Series 2, Issue 3.

Press Information Bureau, Government of India. “New Criminal Laws — Accountability of Police.” Press Release.

Ministry of Home Affairs, Government of India. Lok Sabha Unstarred Question No. 452, answered 2 December 2025.

National Crime Records Bureau. Crime in India 2023 (and preceding annual reports, 2018–2022), Ministry of Home Affairs.

Drishti IAS. “Crime in India 2023 Report.” Daily News Analysis.

The Tribune. “Only 1.6% Conviction Rate in 2 Years Amid Surge in Cybercrime Cases.”

The Tribune. “Murder Cases Dip, Online Cheating & Forgery Spike, Reveals NCRB Data.”

Safer Internet India. “Cybercrimes Up 217% in the Past Five Years: Insights from the NCRB Report.”

Deccan Herald. “Odisha Reports Highest Cases of Cybercrime against Women in 2022: NCRB.”

Wikipedia contributors. “Bharatiya Nyaya Sanhita, 2023” and “Section 63 of the Bharatiya Nyaya Sanhita.”

Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1 (Supreme Court of India).

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (Supreme Court of India).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (Supreme Court of India).

Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185, 2001.