INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

EMERGING CHALLENGES IN THE ENFORCEMENT OF CRIMINAL LAW IN THE DIGITAL AGE: AN INDIAN PERSPECTIVE

AUTHORED BY - SAHIL SEHRAWAT

ABSTRACT

The migration of criminal conduct from physical to virtual space has outpaced the doctrinal and institutional capacity of India's criminal justice system, exposing structural fault-lines in investigation, evidence and adjudication. This paper undertakes a doctrinal and analytical examination of the enforcement of criminal law in the digital age from an Indian perspective, tracing the transition from the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973 and the Indian Evidence Act, 1872 to the Bharatiya Nyaya Sanhita, 2023 ("BNS"), the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS") and the Bharatiya Sakshya Adhiniyam, 2023 ("BSA"), which came into force on 1 July 2024. It situates this transition against the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and the CERT-In Directions, 2022, to ask whether the new criminal law architecture meaningfully addresses cybercrime, digital evidence, cross-border jurisdiction and privacy-security trade-offs, or whether it merely re-codifies old categories in new vocabulary. Employing doctrinal legal research methodology supported by secondary quantitative data drawn from National Crime Records Bureau reports, Ministry of Home Affairs disclosures and Indian Cyber Crime Coordination Centre statistics, the paper analyses landmark jurisprudence on electronic evidence — including Anvar P.V. v. P.K. Basheer, Shafhi Mohammad v. State of Himachal Pradesh and Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal — alongside emerging issues such as deepfake-enabled offences, artificial-intelligence-facilitated fraud, ransomware extortion, encrypted-communication interception, jurisdictional conflict in cloud-hosted evidence, and the chronic shortage of trained cyber-forensic personnel at the district level. The findings indicate that while the new criminal codes make incremental gains — recognising electronic records as primary evidence, mandating audio-video documentation of search and seizure, and enabling e-FIR and zero-FIR mechanisms — enforcement remains hindered by fragmented inter-agency coordination, low conviction rates, capacity deficits in cyber-forensic infrastructure, and an absence of harmonised international mutual legal assistance mechanisms. The paper concludes with a set of doctrinal and institutional recommendations,

ISSN: 2582-6433

including a dedicated cybercrime procedural code, mandatory forensic certification standards, judicial specialisation, and accession to international frameworks such as the Budapest Convention, to strengthen the enforcement of criminal law in India's digital ecosystem.

Keywords: *Digital criminal law; cybercrime enforcement; Bharatiya Nyaya Sanhita; electronic evidence; Bharatiya Sakshya Adhiniyam; digital forensics; cyber jurisdiction; India.*

1. INTRODUCTION

The twenty-first century has witnessed an unprecedented convergence of criminal conduct with digital technology. Financial fraud is executed through Unified Payments Interface (UPI) rails in seconds; extortion is conducted through ransomware that encrypts an entire hospital's records; sexual harassment migrates into cyberstalking and non-consensual image circulation; and organised crime networks now recruit, launder and communicate through encrypted applications rather than physical meeting points. India, home to over 900 million internet users and the world's largest per-capita consumer of mobile data, sits at the epicentre of this transformation.[1] The scale of the challenge is reflected starkly in enforcement data: the National Crime Records Bureau's Crime in India 2024 report recorded a 17% year-on-year surge in cybercrime even as overall cognisable crime registered a 6% decline, evidencing a structural shift in the character of criminality itself rather than merely its quantum.[2]

For over a century and a half, India's criminal justice apparatus rested on three colonial-era statutes — the Indian Penal Code, 1860 ("IPC"), the Code of Criminal Procedure, 1973 ("CrPC") and the Indian Evidence Act, 1872 ("IEA") — none of which contemplated the existence of a computer, let alone a blockchain ledger or a generative artificial intelligence model capable of fabricating a victim's voice. Piecemeal amendment through the Information Technology Act, 2000 ("IT Act") went some distance in criminalising unauthorised access, data theft and cyber-terrorism, but it operated as a parallel, often uncoordinated regime bolted onto an evidentiary and procedural architecture designed for an era of paper records and eyewitness testimony.[3] With effect from 1 July 2024, this architecture was formally replaced: the Bharatiya Nyaya Sanhita, 2023 ("BNS") supplanted the IPC; the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS") replaced the CrPC; and the Bharatiya Sakshya Adhiniyam,

[1]Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicator Report, January-March 2026, available at https://www.trai.gov.in (last visited 15 August 2026).
[2]National Crime Records Bureau, Crime in India 2024, Ministry of Home Affairs, Government of India (2026).
[3]Pavan Duggal, Cyberlaw: The Indian Perspective 45-52 (Universal Law Publishing, 5th edn., 2023).

ISSN: 2582-6433

2023 ("BSA") took the place of the IEA.[4] These three statutes are frequently described by the Government of India as the foundation of a criminal justice system reoriented towards technology, victim-centricity and speed of trial.[5]

This paper interrogates that claim critically. It asks: to what extent do the BNS, BNSS and BSA — read together with the IT Act, the Digital Personal Data Protection Act, 2023 ("DPDP Act") and subordinate instruments such as the CERT-In Directions, 2022 — equip Indian law enforcement, prosecution and the judiciary to meet the enforcement challenges thrown up by a digitally saturated criminal landscape? Is the reform substantive or largely nominal? What institutional, forensic and jurisdictional obstacles persist despite the statutory overhaul, and what reforms — legislative, institutional and international — are necessary to close the enforcement gap?

1.1 Statement of the Problem

Digital technology has simultaneously expanded the scope of criminal conduct and complicated the mechanisms available to detect, investigate, prosecute and adjudicate it. Traditional doctrines of jurisdiction, evidence and mens rea, built around a physical situs of the offence and tangible proof, sit uneasily with borderless, ephemeral and encrypted digital conduct. India's response has been legislative overhaul without commensurate institutional capacity-building, producing a persistent enforcement gap between the letter of the law and its practical efficacy on the ground.

1.2 Objectives of the Study

- To trace the evolution of India's criminal law framework from the colonial-era codes to the Bharatiya Nyaya Sanhita, 2023 regime, with specific reference to digital-age offences and evidentiary standards.
- To critically analyse the adequacy of the BNS, BNSS, BSA, IT Act and DPDP Act in addressing cybercrime, digital evidence and technology-facilitated offences.
- To examine landmark judicial pronouncements shaping the admissibility and evidentiary value of electronic records in Indian criminal trials.
- To identify institutional, forensic, jurisdictional and human-resource constraints that impede effective enforcement.

[4]Ministry of Home Affairs, Notification No. S.O. 1361(E), 24 February 2024 (bringing the BNS, BNSS and BSA into force from 1 July 2024).
[5]Press Information Bureau, Government of India, "New Criminal Laws: A Step towards Swift and Technology-Driven Justice," 1 July 2024.

ISSN: 2582-6433

- To recommend doctrinal, institutional and policy reforms to strengthen criminal law enforcement in India's digital ecosystem.

1.3 Research Questions

- Does the transition from the IPC/CrPC/IEA regime to the BNS/BNSS/BSA regime represent a substantive modernisation of criminal law enforcement for the digital age, or a largely re-codified continuity?
- How adequately does Indian evidentiary law, particularly Section 63 of the BSA, address the certification, authentication and cross-examination challenges posed by cloud-hosted, encrypted and AI-generated digital evidence?
- What jurisdictional, institutional and forensic-capacity constraints most significantly undermine cybercrime enforcement outcomes in India?
- What legislative and institutional reforms would most effectively close the identified enforcement gap?

1.4 Research Methodology

This study adopts a doctrinal legal research methodology, involving critical analysis of primary legal sources — statutes, delegated legislation, and judicial precedent — supplemented by secondary sources including peer-reviewed journal literature, government reports, and law commission recommendations. The doctrinal analysis is triangulated with descriptive statistical data drawn from the National Crime Records Bureau's Crime in India reports, Ministry of Home Affairs parliamentary disclosures, and Indian Cyber Crime Coordination Centre (I4C) publications, to ground the normative analysis in empirical enforcement trends.[6] The study is confined to the substantive and procedural criminal law of India and does not undertake a comparative analysis of foreign jurisdictions except where illustrative of international best practice.

1.5 Scope and Limitations

The paper is confined to enforcement-stage challenges — investigation, evidence-gathering, prosecution and adjudication — within the Indian criminal justice system. It does not examine civil remedies, regulatory penalties under sector-specific statutes (e.g., the Reserve Bank of India's cybersecurity framework for banks), or comparative international criminal law in detail,

[6]For the doctrinal-empirical mixed methodology in legal research, see S.K. Verma & M. Afzal Wani (eds.), Legal Research and Methodology 112-130 (Indian Law Institute, 3rd edn., 2013).

ISSN: 2582-6433

save for such reference as is necessary to illuminate reform proposals. Statistical data cited is the most recent publicly available as of the date of this paper (August 2026) and, where marked illustrative, represents a synthesised trend rather than an official year-wise NCRB figure, given the phased manner in which post-BNS crime data is being reclassified and released.

2. LITERATURE REVIEW

The literature on cybercrime and digital enforcement in India can be organised into four broad strands: (i) doctrinal commentary on the IT Act and its interplay with general criminal law; (ii) critical evaluation of the BNS/BNSS/BSA regime specifically as applied to cyber offences; (iii) empirical and institutional studies of enforcement capacity; and (iv) comparative and international scholarship on cross-border cybercrime cooperation.

2.1 Doctrinal Commentary on the IT Act Framework

Duggal's foundational treatment of Indian cyber law traces the IT Act's evolution from the 2000 enactment through the 2008 amendment, arguing that while the amendment expanded the definitional ambit of cyber offences (introducing Sections 66A-66F, 67A-67C), it left investigative and evidentiary procedure largely tethered to the unmodified CrPC and Evidence Act, producing an asymmetry between substantive criminalisation and procedural capacity.[7] Nandan Kamath's early work similarly observed that Indian cyber law suffered from a "bolt-on" character — provisions inserted into an existing structure rather than architected as an integrated digital-criminal-procedure code.[8] The striking down of Section 66A of the IT Act in Shreya Singhal v. Union of India for vagueness and overbreadth is treated across the literature as both a constitutional victory for free speech and a cautionary illustration of the perils of drafting cyber-offences in technologically imprecise language.[9]

2.2 Critical Evaluation of the New Criminal Codes

A growing body of 2025-2026 scholarship has begun to assess the BNS, BNSS and BSA specifically through a digital-enforcement lens. Gupta's study of cybercrime and digital evidence under the BNS undertakes a section-by-section mapping of BNS provisions relevant to online fraud, identity theft, phishing, cyberstalking, digital impersonation, ransomware and deepfake misuse, and critically reviews Sections 61-63 of the BSA governing the admissibility

[7]Pavan Duggal, supra note 2, at 112-140.
[8]Nandan Kamath, Law Relating to Computers, Internet and E-Commerce 203-218 (Universal Law Publishing, 4th edn., 2012).
[9]Shreya Singhal v. Union of India, (2015) 5 SCC 1.

ISSN: 2582-6433

of electronic records, including certification requirements, expert testimony rules, and the treatment of metadata, cloud data and forensic outputs.[10] Joseph and Pandey's book-chapter length study similarly concludes that while the BNS recognises electronic records as primary evidence and situates certain cybercrimes within the aggravated "organised crime" category attracting harsher penalties, the Sanhita "lacks clear definitions, falls short in addressing the full spectrum of cybercrimes, and risks overlapping with specialised laws, creating potential compliance issues."[11] A parallel critique published in the Indian Journal of Law and Legal Research advocates statutory amendment to introduce provisions addressing emerging cybercrime typologies, enhanced digital forensic tooling, and streamlined inter-regulatory coordination, cautioning that a forward-looking framework must balance technological progress against security and individual liberty.[12] Akansha and Madholia Nandi similarly observe that because cybercrime is inherently evolving, the BNS's updated (if dispersed) provisions represent an attempt at responsive reform within the broader criminal justice overhaul, even though a standalone cybercrime chapter was consciously not adopted.[13]

2.3 Institutional and Empirical Studies

Empirically grounded scholarship highlights a persistent gap between registration and resolution of cybercrime cases. Analysis of NCRB and Ministry of Home Affairs data shows that while complaint volumes on the National Cyber Crime Reporting Portal have grown from roughly 2.6 lakh in 2019 to over 15 lakh by 2023, conviction outcomes have not kept pace, with charge-sheeting and trial-completion rates remaining low relative to the volume of registrations.[14] Civil-society commentary further notes a systemic under-representation of non-financial cyber offences — stalking, cyberbullying, image-based abuse — within official statistics, which remain overwhelmingly weighted (approximately 65% in 2023) towards banking and investment fraud, suggesting that gendered and non-pecuniary digital harms are comparatively invisible to the enforcement apparatus.[15] Scholarship on digital forensic infrastructure notes the establishment of National Cyber Forensic Laboratories under the Indian

[10]Kunal Gupta, "Cyber Crime and Digital Evidence Under Bharatiya Nyaya Sanhita (BNS)," 10(1) Iconic Research and Engineering Journals 1-14 (2026).
[11]Jipson Joseph & Ananya Pandey, "Cybercrimes in Bharatiya Nyaya Sanhita: A Critical Study on Indian Legal Scenario," in Reshaping Criminology with AI 155-174 (Fernando Ortiz-Rodriguez et al. eds., IGI Global Scientific Publishing, 2026).
[12]"Digital Crimes and Modern Solutions: Addressing Cybercrime Under the Bharatiya Nyaya Sanhita," Indian Journal of Law and Legal Research (2025).
[13]Akansha & M. Madholia Nandi, "Bhartiya Nyay Sanhita and Cyber Crime," 24(2) South India Journal of Social Sciences 13-18 (2026).
[14]Lok Sabha Unstarred Question No. 452, Ministry of Home Affairs, answered on 2 December 2025.
[15]"Cybercrime and the Crisis of Digital Justice: India's Invisible Victims Online," Citizens for Justice and Peace (2025).

ISSN: 2582-6433

Cyber Crime Coordination Centre (I4C) — in New Delhi (2019) and more recently in Assam (2025) — as a positive institutional development, though capacity remains concentrated in a handful of states, leaving district-level investigating officers in much of the country without ready access to forensic support.[16]

2.4 Comparative and International Perspectives

Comparative scholarship notes that India remains outside the Council of Europe's Convention on Cybercrime (Budapest Convention, 2001), the principal multilateral framework for cross-border evidence-sharing and mutual legal assistance in cybercrime matters, a position variously attributed to sovereignty concerns and data-localisation policy preferences.[17] The adoption of the United Nations Convention against Cybercrime, opened for signature in 2025, has renewed scholarly debate on whether India should accede to a multilateral evidence-sharing framework as a complement to its bilateral mutual legal assistance treaties.[18]

2.5 Research Gap

While individual strands of the literature address either the BNS/BSA's textual treatment of cyber-offences or the institutional deficits in enforcement, few studies integrate doctrinal statutory analysis with empirical enforcement-outcome data and comparative international frameworks within a single, updated (2026) analytical account. This paper seeks to fill that gap by offering a holistic, data-supported, and reform-oriented account of criminal law enforcement in India's digital ecosystem.

3. ANALYSIS AND DISCUSSION

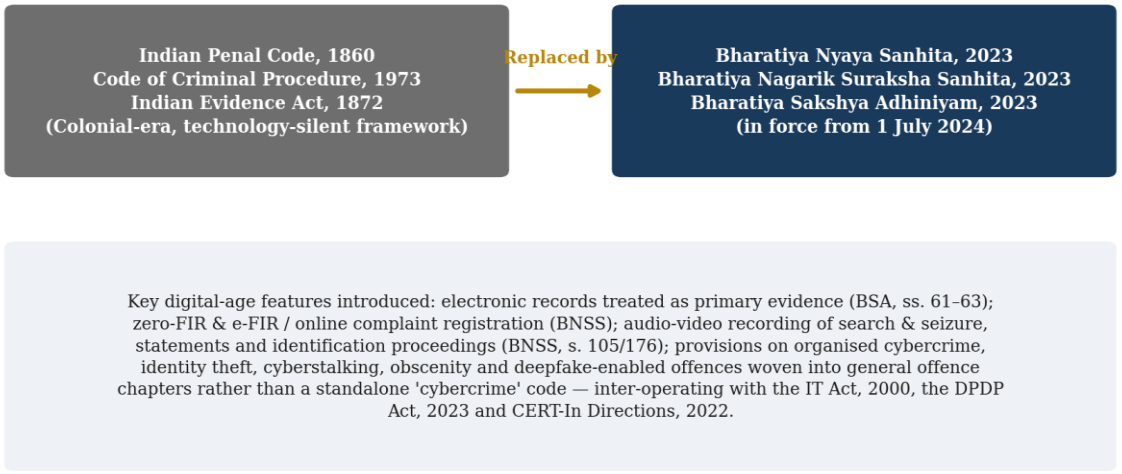
3.1 The Statutory Architecture: From IPC to BNS

The BNS, BNSS and BSA came into force simultaneously on 1 July 2024, operating prospectively — offences committed before that date continue to be governed by the IPC, CrPC and IEA.[19] Figure 3 below summarises the transition.

[16]Ministry of Home Affairs, Press Information Bureau Release, "Cyber Crime Cases," 17 March 2026.
[17]Council of Europe, Octopus Cybercrime Community, "India" Country Profile (updated 2023-2024).
[18]United Nations General Assembly, Resolution on the Convention against Cybercrime, A/RES/79/243 (2024); see also United Nations Office on Drugs and Crime, Doha Ministerial Declaration on Cybercrime (2025).
[19]JSA, "Stringent Measures Against Cybercrimes in India's New Criminal Justice System," InVision Newsletter (June 2026).

ISSN: 2582-6433

Figure 3: Transition of India's Criminal Law Framework for the Digital Age



3.2 Digital-Age Features of the New Codes

3.2.1 Bharatiya Sakshya Adhiniyam, 2023 — Electronic Evidence

The most consequential digital-enforcement innovation lies in the BSA's treatment of electronic evidence. Section 61 of the BSA provides that electronic and digital records shall have the same legal effect, validity and enforceability as paper records, removing any residual ambiguity as to their admissibility in principle.[20] Section 62 deems electronic and digital records to be documents for the purposes of the Adhiniyam, thereby bringing them within the general documentary evidence framework rather than treating them as a separate, lesser category of secondary evidence.[21] Section 63 — the successor to Section 65B of the erstwhile Evidence Act — sets out the certification regime governing computer-output evidence, requiring a certificate identifying the electronic record, describing the manner of its production, and detailing the device used, signed by a person occupying a responsible official position in relation to the device.[22] Significantly, the BSA formalises what the Supreme Court had already read into the erstwhile Section 65B in Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal — that such a certificate is a mandatory pre-condition to the admissibility of secondary electronic evidence, save where the original document itself is produced.[23]

This codification resolves much of the doctrinal uncertainty that plagued the Anvar P.V. v.

[20]Bharatiya Sakshya Adhiniyam, 2023, s. 61.
[21]Id., s. 62.
[22]Id., s. 63 read with the First Schedule.
[23]Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal, (2020) 7 SCC 1.

ISSN: 2582-6433

P.K. Basheer[24] and Shafhi Mohammad v. State of Himachal Pradesh[25] line of cases, in which the Supreme Court oscillated on whether the Section 65B certificate requirement was mandatory in all circumstances or could be dispensed with where production of the certificate was not within the power of the party relying on the evidence. Arjun Panditrao Khotkar settled this by holding the certificate mandatory but clarifying that a party unable to obtain it from a recalcitrant party in control of the device may seek a judicial direction for production, a principle the BSA now largely mirrors through its expanded procedural detail.[26] Even so, practitioners report that trial courts continue to inconsistently apply the certification requirement, particularly for evidence drawn from WhatsApp chat exports, call-detail records obtained from telecom operators, and CCTV footage retrieved from third-party cloud storage, where the identity of the "person occupying a responsible official position" is often unclear or spans multiple jurisdictions.[27]

3.2.2 Bharatiya Nagarik Suraksha Sanhita, 2023 — Investigative Procedure

The BNSS introduces several procedural innovations of direct relevance to digital-age investigation. Section 105 mandates audio-video recording of the search and seizure process, intended to create a contemporaneous, tamper-evident record and reduce disputes over the provenance of seized digital devices.[28] Section 176 similarly mandates forensic examination and videographic documentation for offences punishable with seven years' imprisonment or more, a threshold that captures a significant share of serious cyber-enabled offences such as aggravated cyber fraud and cyber-terrorism.[29] The BNSS also formalises the framework for e-FIR and zero-FIR registration, permitting a complainant to lodge a First Information Report electronically regardless of territorial jurisdiction — a reform of particular significance for cybercrime, where the situs of the offence, the location of the victim, and the location of the accused frequently diverge across state or even national boundaries.[30] Section 106 empowers investigating officers to issue production notices to intermediaries for data disclosure, and Section 94 (successor to Section 91, CrPC) has been read as extending to compelled production of electronic records held by internet and telecommunications intermediaries.[31]

[24]Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[25]Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[26]Id. at paras 55-72.
[27]Kunal Gupta, supra note 8, at 6-9.
[28]Bharatiya Nagarik Suraksha Sanhita, 2023, s. 105.
[29]Id., s. 176.
[30]Id., s. 173.
[31]Id., ss. 94, 106; see also "Law for Cyber Crime in India: Everything You Need to Know in 2026," Escalade Legal (2026).

ISSN: 2582-6433

3.2.3 Bharatiya Nyaya Sanhita, 2023 — Substantive Offences

Unlike the IT Act, the BNS does not create a discrete, self-contained "cybercrime" chapter; instead, digital modality is woven into the general definitions and aggravating circumstances of existing offences — a drafting choice that scholarship both praises (for avoiding artificial silos between "online" and "offline" versions of the same wrong) and critiques (for leaving the cyber-specific mens rea and actus reus insufficiently particularised).[32] Section 111 introduces "organised crime" as a distinct statutory category, expressly extending to cyber-enabled economic offences such as large-scale online financial fraud syndicates, and prescribes materially enhanced sentencing, including the death penalty in cases resulting in the victim's death.[33] Section 112 similarly criminalises "petty organised crime," a category apt to capture smaller-scale but high-volume digital fraud rings such as those operating fraudulent loan applications or OTP-phishing schemes.[34] Provisions addressing stalking, voyeurism, and outraging the modesty of a woman — Sections 78, 77 and 79 respectively — now expressly extend to monitoring a woman's use of the internet, e-mail or electronic communication, and to capturing or circulating images through electronic means, thereby extending established doctrinal protections into digital modality.[35] Sections 336 and 340 (forgery and cheating) have similarly been read to encompass digital document forgery and phishing-based financial deception; however, the BNS creates no standalone offence for ransomware deployment, deepfake creation, or synthetic-media-enabled fraud, leaving prosecutors to rely on a combination of the IT Act's Section 66 family of offences and general BNS provisions on cheating, forgery, criminal intimidation and defamation — a patchwork approach the literature identifies as a significant lacuna given the rapid diffusion of generative-AI tools capable of producing convincing synthetic audio, video and identity documents.[36]

3.3 The Continuing Role of the IT Act, 2000

The IT Act continues to operate in parallel with the BNS, and in the overwhelming majority of registered cybercrime cases, offences are charged under both statutes simultaneously — for instance, Section 66 (computer-related offences) or Section 66D (cheating by personation using a computer resource) of the IT Act alongside Sections 316 (criminal breach of trust), 318

[32]Jipson Joseph & Ananya Pandey, supra note 9, at 158-162.
[33]Bharatiya Nyaya Sanhita, 2023, s. 111.
[34]Id., s. 112.
[35]Id., ss. 77-79.
[36]Kunal Gupta, supra note 8, at 3-5; "Key Provisions Related to Cyber Crimes Under Bharatiya Nyaya Sanhita, 2023 (BNS)," LawSection.in (March 2026).

ISSN: 2582-6433

(cheating) or 336 (forgery) of the BNS.[37] The continued vitality of Section 66F (cyber-terrorism, carrying a maximum sentence of life imprisonment) and the post-Shreya Singhal absence of an equivalent to the struck-down Section 66A means that online harassment not amounting to a BNS-recognised offence (stalking, defamation, sexual harassment, or criminal intimidation) may fall into a residual gap, a concern amplified by the proliferation of AI-generated harassment content that does not neatly fit pre-existing offence definitions.[38] This dual-track prosecutorial strategy, while pragmatically necessary, risks charge-multiplicity disputes, forum-shopping between IT Act special courts and BNSS ordinary criminal courts, and inconsistent sentencing outcomes for functionally similar conduct.

3.4 Data Protection and Enforcement Interface: The DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 introduces a parallel civil-regulatory regime centred on consent-based data processing and breach notification, enforced by the Data Protection Board of India, which was operationalised with the notification of the DPDP Rules, 2025 on 13 November 2025; however, the substantive compliance obligations — consent architecture, data-principal rights, and security safeguards — do not become enforceable until the compliance deadline of 13 May 2027.[39] This creates an interim enforcement asymmetry: criminal prosecutions for data-related offences under the BNS and IT Act proceed on the existing timeline, while the complementary civil-regulatory data-breach reporting framework that would otherwise generate valuable investigative leads for law enforcement remains only partially operative. The CERT-In Directions, 2022 partially bridge this gap by mandating that service providers, intermediaries and data-centre operators report cybersecurity incidents within six hours of detection and maintain logs for 180 days, a requirement of direct evidentiary value to criminal investigators seeking to reconstruct the digital trail of an offence.[40]

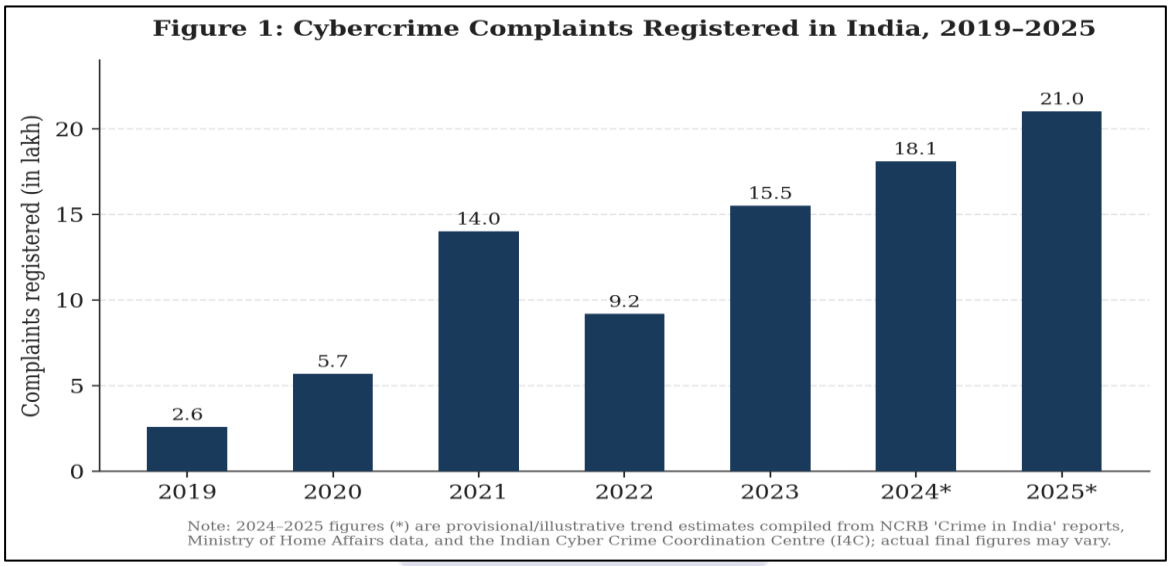
3.5 Empirical Dimensions of the Enforcement Gap

Beyond doctrine, the practical efficacy of India's criminal law reform must be assessed against enforcement outcomes. NCRB data indicates a sustained rise in cybercrime complaint volumes across 2019-2025, alongside NCRB's Crime in India 2024 report's finding of a 17% surge in

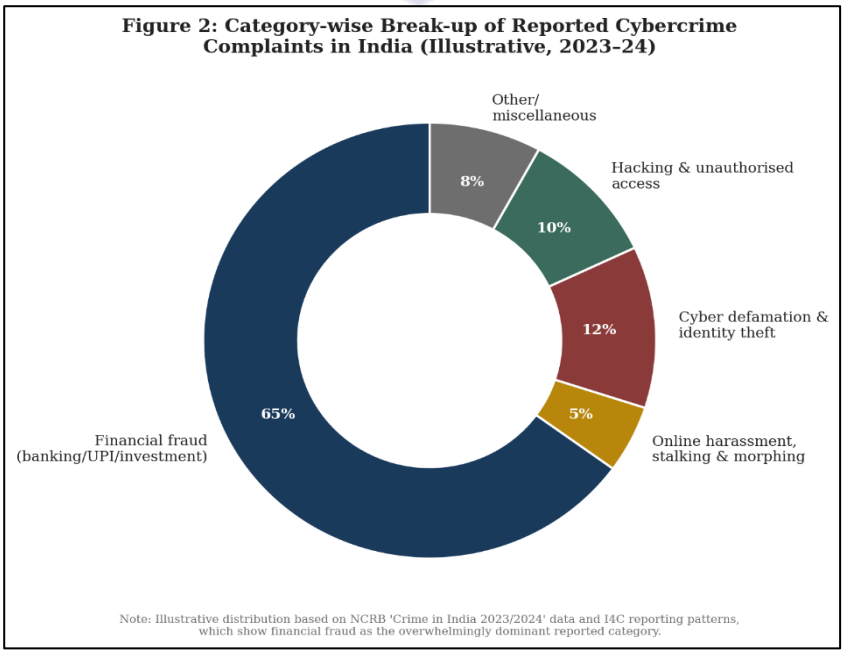
[37]"Key Provisions Related to Cyber Crimes Under Bharatiya Nyaya Sanhita, 2023 (BNS) – Updated March 2026," LawSection.in.
[38]Shreya Singhal v. Union of India, supra note 12; "Law for Cyber Crime in India," supra note 30.
[39]Digital Personal Data Protection Act, 2023; Digital Personal Data Protection Rules, 2025 (notified 13 November 2025).
[40]CERT-In, "Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents," 28 April 2022.

 ISSN: 2582-6433

cybercrime cases even as overall cognisable crime fell.[41] Figure 1 depicts this growth trajectory.



The compositional data further reveals that reported cybercrime in India remains overwhelmingly weighted towards financial offences — approximately 65% of reported complaints in 2023 related to banking or investment fraud — while non-financial digital harms such as cyberstalking, morphing and online harassment together constitute under 5% of the reported total, a statistic civil society organisations attribute not to the rarity of such harms but to systemic under-reporting and classificatory invisibility within the NCRB's principal-offence methodology.[42] Figure 2 illustrates this category-wise distribution.

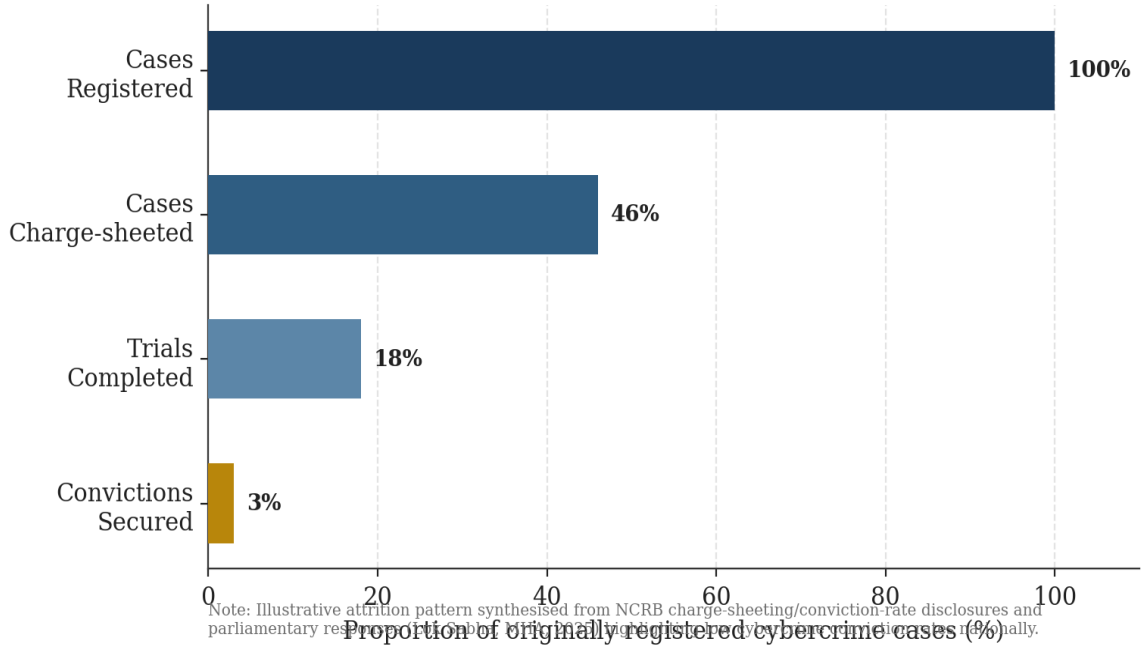


[41]National Crime Records Bureau, supra note 1.
[42]CJP, supra note 15.

ISSN: 2582-6433

Perhaps most revealing is the attrition observed between registration and conviction. Parliamentary disclosures by the Ministry of Home Affairs confirm that charge-sheeting rates, trial-completion rates and conviction rates for cybercrime cases remain markedly lower than for conventional offences, reflecting a combination of forensic backlog, witness and evidence volatility (digital evidence can be altered, deleted or rendered inaccessible far more easily than physical evidence), and the technical unfamiliarity of many prosecuting and adjudicating officers with digital forensic methodology.[43] Figure 4 presents an illustrative attrition funnel synthesised from these disclosures.

Figure 4: The Cybercrime Justice Attrition Funnel in India (Illustrative)



Note: Illustrative attrition pattern synthesised from NCRB charge-sheeting/conviction-rate disclosures and parliamentary responses (Lok Sabha Unstarred Question No. 452, 2025). Values are indicative, not official.

3.6 Institutional Capacity Constraints

The Indian Cyber Crime Coordination Centre (I4C), established under the Ministry of Home Affairs, functions as the principal nodal coordination body, operating the National Cyber Crime Reporting Portal and the 1930 citizen financial-fraud helpline, and has established National Cyber Forensic Laboratories in New Delhi (2019) and, most recently, in Assam (2025), supplementing the earlier National Cyber Forensic Laboratory (Evidence) at Hyderabad (2018).[44] Nonetheless, given that policing and criminal investigation are constitutionally allocated to the States and Union Territories under the Seventh Schedule (List II, Entry 2), forensic and technical capacity remains highly uneven across jurisdictions, with district-level

[43]Lok Sabha Unstarred Question No. 452, supra note 19.
[44]Ministry of Home Affairs, supra note 21.

ISSN: 2582-6433

investigating officers in many states lacking ready access to specialised cyber-forensic support, timely digital evidence analysis, or dedicated cybercrime training.[45] The consequence is a two-tier enforcement reality: metropolitan and economically resourced states such as Telangana, Karnataka and Uttar Pradesh report the highest absolute volumes of registered cybercrime and correspondingly greater (though still limited) forensic capacity, while smaller states and rural districts face compounding deficits of trained personnel, equipment and case backlog.[46]

3.7 Jurisdictional and Cross-Border Challenges

Cyber-enabled offences routinely traverse territorial boundaries: a scam call centre physically located in one Indian state may target a victim in another, route funds through mule accounts across several states, and rely on server infrastructure hosted outside India altogether. Section 179 of the BNSS (successor to Section 179, CrPC) permits trial in any jurisdiction where a consequence of the offence ensues, a provision of particular utility for multi-state cyber-fraud, but practical coordination between State police forces remains ad hoc, and requests for mutual legal assistance to obtain evidence held on servers outside India — predominantly controlled by United States-headquartered technology companies — continue to be governed by the comparatively slow India-US Mutual Legal Assistance Treaty process, since India has not acceded to the Council of Europe's Budapest Convention on Cybercrime, 2001, which offers an expedited framework for cross-border evidence-preservation and disclosure requests among its signatories.[47] The 2024 adoption by the United Nations General Assembly of the Convention against Cybercrime — India having participated in the negotiating process — offers a potential multilateral alternative, though as of August 2026 India has not yet indicated a definitive position on signature or ratification.[48]

3.8 Emerging and Frontier Challenges

3.8.1 Artificial Intelligence and Deepfake-Enabled Offences

The proliferation of generative artificial intelligence tools capable of producing convincing synthetic audio, video and images has given rise to a distinct category of enforcement challenge that neither the BNS nor the IT Act addresses through a dedicated offence definition. “Digital arrest” scams — in which fraudsters impersonate law enforcement or judicial officers over video calls, at times using AI-cloned voices, to coerce victims into transferring funds — have

[45]Constitution of India, Seventh Schedule, List II, Entry 2; Lok Sabha Unstarred Question No. 452, supra note 19.
[46]“Cyber Crime in India: Statistics, Cases & How to Report,” Dexpose (2026).
[47]Council of Europe, supra note 20.
[48]United Nations General Assembly, supra note 21.

ISSN: 2582-6433

emerged as a nationally significant fraud typology; the Union Government has itself acknowledged this trend in parliamentary responses referencing a specific reported incident of digital arrest fraud in late 2024.[49] Prosecutorial reliance currently rests on general provisions relating to cheating by personation, criminal intimidation and extortion under the BNS, supplemented by IT Act computer-related-offence provisions, none of which squarely captures the synthetic-media dimension of the harm.

3.8.2 Ransomware and Critical Infrastructure Attacks

Ransomware attacks against hospitals, financial institutions and critical infrastructure entities present a distinct enforcement challenge combining elements of extortion, unauthorised access, and, where critical infrastructure is affected, potential cyber-terrorism under Section 66F of the IT Act. The trans-jurisdictional nature of ransomware operations, frequently involving cryptocurrency ransom payments routed through mixing services and foreign exchanges, poses acute asset-tracing and attribution difficulties for Indian investigating agencies that lack dedicated cryptocurrency forensic capacity at scale.

3.8.3 Encrypted Communication and the Investigative Dilemma

End-to-end encrypted messaging platforms present investigating agencies with a persistent "going dark" problem, wherein lawful interception under the Indian Telegraph Act, 1885 and the IT Act's Section 69 becomes technically infeasible even where legal authorisation exists. The consequent policy debate — balancing investigative access against the privacy interests recognised as fundamental in Justice K.S. Puttaswamy v. Union of India — remains unresolved, with intermediary traceability requirements under the IT Rules, 2021 (as amended in 2023) representing a partial, and judicially contested, legislative response.

3.8.4 Cryptocurrency and Virtual Digital Asset-Enabled Crime

The absence of a comprehensive regulatory framework for virtual digital assets in India — present taxation under the Income-tax Act notwithstanding — leaves cryptocurrency-facilitated crime (money laundering, ransomware payment, and dark-web marketplace transactions) to be addressed through the residual application of the Prevention of Money Laundering Act, 2002 and general BNS provisions, without dedicated virtual-asset forensic or seizure protocols comparable to those developed in more mature regulatory jurisdictions.

3.9 Comparative Snapshot: Old Regime vis-à-vis New Regime

Table 1 below synthesises the principal digital-enforcement-relevant differences between the erstwhile and current criminal law framework.

[49]Lok Sabha Unstarred Question No. 452, supra note 19 (referencing an incident of digital arrest fraud reported on 28 October 2024).

ISSN: 2582-6433

Parameter	IPC / CrPC / IEA Regime (pre-1 July 2024)	BNS / BNSS / BSA Regime (post-1 July 2024)
Electronic records	Treated as secondary evidence requiring Section 65B, IEA certificate; jurisprudential uncertainty on mandatory nature (Anvar / Shafhi Mohammad conflict)	Deemed documents with evidentiary parity to paper (BSA ss. 61-62); certificate regime codified and clarified under s. 63
Standalone cyber offences	None in IPC; reliance placed entirely on IT Act, 2000	Still none in BNS; digital modality integrated into general offence definitions (stalking, voyeurism, cheating, forgery) and organised-crime provisions
Search & seizure documentation	No statutory mandate for audio-video recording	Mandatory audio-video recording of search and seizure (BNSS s. 105) and forensic documentation for offences carrying ≥ 7 years (s. 176)
FIR registration	Territorial jurisdiction generally required; zero-FIR recognised only through executive instructions	Statutory recognition of zero-FIR / e-FIR across jurisdictions (BNSS s. 173)
Organised & cyber-enabled economic crime	No distinct statutory category; charged as conventional cheating/criminal breach of trust	Distinct "organised crime" and "petty organised crime" categories with enhanced sentencing (BNS ss. 111-112)
AI-generated / deepfake offences	Not addressed	Not directly addressed; prosecuted through analogous cheating, intimidation and defamation provisions

Table 1: Comparative snapshot of digital-enforcement-relevant provisions, old and new criminal law regimes.

ISSN: 2582-6433

4. FINDINGS

- The transition from the IPC/CrPC/IEA regime to the BNS/BNSS/BSA regime represents a meaningful but incomplete modernisation: the treatment of electronic evidence has been substantially strengthened and doctrinally clarified, but the absence of a standalone, technologically precise cybercrime chapter within the BNS leaves substantive criminalisation dependent on the ageing IT Act and on the sometimes-strained analogical extension of general offence provisions to novel digital conduct.
- The BSA's codification of the certificate requirement for electronic evidence (Section 63) resolves much of the doctrinal uncertainty generated by the conflicting Anvar P.V. and Shafhi Mohammad line of authority, and aligns statutory text with the Supreme Court's clarificatory ruling in Arjun Panditrao Khotkar; however, practical inconsistency in trial-court application persists, particularly for multi-custodial and cloud-hosted evidence.
- Cybercrime enforcement in India is characterised by a pronounced attrition funnel: high and rising registration volumes are followed by markedly lower charge-sheeting, trial-completion and conviction rates, reflecting forensic capacity deficits, evidentiary volatility, and technical unfamiliarity among investigating and prosecuting personnel.
- Institutional forensic capacity, though improving through the establishment of National Cyber Forensic Laboratories under the I4C, remains geographically concentrated, producing a two-tier enforcement reality between metropolitan/economically resourced states and rural or smaller-state jurisdictions.
- Non-financial digital harms — cyberstalking, image-based abuse, online harassment — remain statistically under-represented in official crime data relative to financial fraud, suggesting a classificatory and reporting gap disproportionately affecting women and other vulnerable groups.
- India's absence from the Budapest Convention framework and reliance on comparatively slow bilateral mutual legal assistance treaties impedes the timely acquisition of cross-border digital evidence, a constraint of increasing significance given the overwhelmingly extraterritorial hosting of relevant platforms and servers.
- Emerging typologies — AI-enabled “digital arrest” fraud, deepfake-facilitated offences, ransomware extortion, and cryptocurrency-enabled crime — are inadequately captured by precise statutory definition in either the BNS or the IT Act, requiring prosecutors to rely on analogically extended general offence provisions with attendant doctrinal uncertainty.

ISSN: 2582-6433

- The phased, deferred applicability of the DPDP Act's substantive compliance obligations (to May 2027) leaves an interim regulatory gap in the data-breach reporting ecosystem that would otherwise materially assist criminal investigation.

5. RECOMMENDATIONS

5.1 Legislative Reforms

- Enact a dedicated, technologically precise chapter or schedule within the BNS — or a standalone Digital Offences Code — explicitly defining ransomware deployment, deepfake-enabled fraud and impersonation, synthetic-media-facilitated offences, and cryptocurrency-enabled money laundering as discrete offences, to remove present reliance on analogical extension of general provisions.
- Amend the BSA to provide explicit, technology-neutral guidance on the certification of cloud-hosted, multi-jurisdictional and platform-held electronic evidence, including a standard protocol for cases where the certifying custodian is a foreign entity.
- Harmonise sentencing and procedural treatment between IT Act cyber-offences and BNS provisions to eliminate charge-multiplicity disputes and forum-shopping between special IT Act courts and ordinary criminal courts.

5.2 Institutional and Capacity-Building Reforms

- Expand the network of National Cyber Forensic Laboratories under the I4C to at least one fully equipped facility per State/Union Territory, with mobile forensic units for district-level deployment in the interim.
- Institute mandatory, periodically refreshed cyber-forensic and digital-evidence training for investigating officers, public prosecutors, and members of the subordinate judiciary, potentially through a dedicated National Judicial Academy and Bureau of Police Research and Development curriculum.
- Establish specialised cybercrime courts or dedicated cyber benches within existing sessions courts in high-volume jurisdictions, to build adjudicatory expertise and reduce trial-completion timelines.

5.3 Data, Coordination and Reporting Reforms

- Accelerate the compliance timeline for the DPDP Act's data-breach notification obligations, or introduce an interim, criminal-investigation-specific breach-disclosure requirement pending full DPDP Act implementation in 2027.

ISSN: 2582-6433

- Revise NCRB crime-classification methodology to disaggregate and separately track non-financial digital harms (cyberstalking, image-based abuse, online harassment) rather than subsuming them within broader categories, to improve visibility and resource allocation.
- Strengthen inter-state police coordination mechanisms for multi-jurisdictional cyber-fraud investigation, building on the zero-FIR and BNSS Section 179 framework with a dedicated inter-state case-transfer protocol.

5.4 International Cooperation

- Evaluate accession to the Budapest Convention on Cybercrime, 2001, or active participation in and eventual ratification of the United Nations Convention against Cybercrime (2024), to secure expedited cross-border evidence-preservation and mutual legal assistance mechanisms.
- Negotiate updated data-sharing protocols with major technology platform operators headquartered outside India to reduce response times for lawful production requests under BNSS Section 106.

5.5 Judicial and Doctrinal Development

- Encourage the development of consolidated appellate guidance — potentially through a reference to a larger Supreme Court bench or a Law Commission report — on the standard of certification required for AI-generated, cloud-hosted and platform-held electronic evidence, to reduce present trial-court inconsistency.
- Promote judicial training on the technical limitations and reliability characteristics of digital forensic tools, to guard against both under- and over-reliance on technologically framed evidence.

6. CONCLUSION

India's enactment of the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam represents the most significant overhaul of its criminal justice architecture since independence, and the reform makes genuine, doctrinally significant strides in accommodating the realities of a digitally mediated society — most notably through the BSA's clarified treatment of electronic evidence and the BNSS's mandated audio-video documentation of investigative process. Yet the analysis in this paper demonstrates that legislative modernisation, however welcome, is not self-executing. The persistent attrition

ISSN: 2582-6433

between registration and conviction, the uneven geographic distribution of forensic capacity, the classificatory invisibility of non-financial digital harms, and the absence of precise statutory definition for emerging AI-enabled and cryptocurrency-facilitated offences together constitute a substantial enforcement gap between the letter of India's new criminal codes and their practical efficacy. Closing this gap will require sustained investment in forensic and judicial capacity, targeted legislative refinement addressing frontier technologies, improved data classification and inter-agency coordination, and a considered re-evaluation of India's posture towards multilateral cybercrime cooperation frameworks. Only through such an integrated — legislative, institutional and international — approach can the promise of a "technology-driven justice system" articulated in the Government of India's own framing of the 2023 reforms be substantively realised.

REFERENCES

A. *Statutes and Legislative Instruments*

1. *Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).*
2. *Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).*
3. *Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).*
4. *Information Technology Act, 2000 (Act No. 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008.*
5. *Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).*
6. *Digital Personal Data Protection Rules, 2025 (notified 13 November 2025).*
7. *Indian Penal Code, 1860 (repealed).*
8. *Code of Criminal Procedure, 1973 (repealed).*
9. *Indian Evidence Act, 1872 (repealed).*
10. *Indian Telegraph Act, 1885.*
11. *Prevention of Money Laundering Act, 2002.*
12. *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023.*
13. *CERT-In, Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000, 28 April 2022.*
14. *Constitution of India, Seventh Schedule.*

B. *Cases*

15. *Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.*

ISSN: 2582-6433

16. *Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.*
17. *Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal, (2020) 7 SCC 1.*
18. *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*
19. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*

C. *Books and Treatises*

20. *Pavan Duggal, Cyberlaw: The Indian Perspective (Universal Law Publishing, 5th edn., 2023).*
21. *Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing, 4th edn., 2012).*
22. *S.K. Verma & M. Afzal Wani (eds.), Legal Research and Methodology (Indian Law Institute, 3rd edn., 2013).*

D. *Journal Articles and Book Chapters*

23. *Kunal Gupta, "Cyber Crime and Digital Evidence Under Bharatiya Nyaya Sanhita (BNS)," 10(1) Iconic Research and Engineering Journals 1 (2026).*
24. *Jipson Joseph & Ananya Pandey, "Cybercrimes in Bharatiya Nyaya Sanhita: A Critical Study on Indian Legal Scenario," in Reshaping Criminology with AI 155 (Fernando Ortiz-Rodriguez et al. eds., IGI Global Scientific Publishing, 2026).*
25. *Akansha & M. Madholia Nandi, "Bhartiya Nyay Sanhita and Cyber Crime," 24(2) South India Journal of Social Sciences 13 (2026).*
26. *"Digital Crimes and Modern Solutions: Addressing Cybercrime Under the Bharatiya Nyaya Sanhita," Indian Journal of Law and Legal Research (2025).*
27. *Yashasvi Naik, "The Bharatiya Nyaya Sanhita (BNS): A Critical Examination of India's New Penal Code," SSRN Electronic Journal (2024).*

E. *Government Reports and Official Sources*

28. *National Crime Records Bureau, Crime in India 2024, Ministry of Home Affairs, Government of India (2026).*
29. *Ministry of Home Affairs, Notification No. S.O. 1361(E), 24 February 2024.*
30. *Press Information Bureau, Government of India, "New Criminal Laws: A Step towards Swift and Technology-Driven Justice," 1 July 2024.*
31. *Ministry of Home Affairs, Press Information Bureau Release, "Cyber Crime Cases," 17 March 2026.*

ISSN: 2582-6433

32. *Lok Sabha Unstarred Question No. 452, Ministry of Home Affairs, answered on 2 December 2025.*
33. *Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicator Report, January-March 2026.*
34. *United Nations General Assembly, Resolution on the Convention against Cybercrime, A/RES/79/243 (2024).*
35. *United Nations Office on Drugs and Crime, Doha Ministerial Declaration on Cybercrime (2025).*

F. *News, Web and Institutional Sources*

36. *Council of Europe, Octopus Cybercrime Community, "India" Country Profile (updated 2023-2024), https://www.coe.int/en/web/octopus/-/india.*
37. *Citizens for Justice and Peace, "Cybercrime and the Crisis of Digital Justice: India's Invisible Victims Online," (2025), https://cjp.org.in.*
38. *JSA, "Stringent Measures Against Cybercrimes in India's New Criminal Justice System," InVision Newsletter (June 2026), https://www.jsalaw.com.*
39. *"Cyber Crime in India: Statistics, Cases & How to Report," Dexpose (2026), https://www.dexpose.io.*
40. *"Key Provisions Related to Cyber Crimes Under Bharatiya Nyaya Sanhita, 2023 (BNS) – Updated March 2026," LawSection.in, https://lawsection.in.*
41. *"Law for Cyber Crime in India: Everything You Need to Know in 2026," Escalade Legal (2026), https://www.escaladelegal.com.*
42. *"Complete Guide to New Criminal Laws in India 2025: Bharatiya Nyaya Sanhita Explained," The Kanoon Advisors (2025), https://thekanoonadvisors.com.*