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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

CYBERCRIME INVESTIGATION IN INDIA: EVALUATING THE EFFECTIVENESS OF THE INFORMATION TECHNOLOGY ACT, 2000 AND THE NEW CRIMINAL LAWS

AUTHORED BY - ATUL VERMA

ABSTRACT

The transition of India's criminal justice architecture 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"), with effect from 1 July 2024, has occurred against the backdrop of an unprecedented surge in cybercrime. Ministry of Home Affairs data indicate that cyber-fraud losses reported on the National Cyber Crime Reporting Portal rose from roughly ₹551 crore in 2021 to over ₹22,800 crore in 2024 and ₹22,495 crore in 2025, with complaint volumes crossing 28 lakh cases in a single year. Against this backdrop, this paper undertakes a doctrinal and analytical evaluation of the adequacy of India's cybercrime investigation framework, examining the interplay between the Information Technology Act, 2000 (as amended in 2008) and the newly enacted criminal statutes. The paper traces the substantive offence provisions under Sections 43, 65 to 66F, 67 to 67C, 69 and 70 of the IT Act, juxtaposes them against the cyber-related provisions scattered across the BNS (including Sections 111, 316, 318, 319 and 336), and critically analyses the procedural and evidentiary changes introduced by the BNSS and Section 63 of the BSA, which replaced the much-litigated Section 65B of the Indian Evidence Act. It further examines the institutional architecture comprising the Indian Cyber Crime Coordination Centre, CERT-In and State Cyber Cells, and evaluates jurisdictional and cross-border evidentiary challenges in light of India's continued non-accession to the Budapest Convention and the 2025 United Nations Convention against Cybercrime. Drawing on landmark judicial pronouncements including Shreya Singhal v. Union of India, Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, the paper argues that while the new criminal laws introduce welcome procedural modernisation, the absence of a consolidated cybercrime code, chronic shortages of trained cyber-forensic personnel, and low conviction rates continue to undermine investigative effectiveness. The paper concludes with a set of doctrinal and institutional recommendations for reform.

ISSN: 2582-6433

Keywords: *Cybercrime, Information Technology Act 2000, Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam, Digital Evidence, Cyber Forensics, India*

1. INTRODUCTION

The proliferation of internet penetration, the near-universal adoption of smartphones and Unified Payments Interface (UPI)-based digital transactions, and the accelerated digitisation of governmental and financial services have transformed India into one of the world's largest and most vulnerable digital economies. With more than 86 per cent of households reporting internet access and over ten billion UPI transactions processed monthly, the attack surface available to cyber-offenders has expanded dramatically, extending from metropolitan centres into Tier-2 and Tier-3 towns where digital literacy remains comparatively low.

This expansion of the digital economy has been accompanied by a corresponding and alarming rise in cybercrime. Cybercrime complaints registered on the National Cyber Crime Reporting Portal ("NCRP") grew from approximately 4.5 lakh in 2021 to over 22.68 lakh in 2024 and further to 28.15 lakh in 2025, while reported financial losses rose from roughly ₹551 crore to over ₹22,800 crore over the same period. Investment scams, "digital arrest" extortion, sextortion, deepfake-enabled impersonation, and mule-account based money-laundering networks have emerged as dominant typologies, reflecting the increasing sophistication of transnational cyber-fraud syndicates, several of which operate from scam compounds in South-East Asia.

India's principal legislative response to cybercrime has, since the turn of the millennium, been the Information Technology Act, 2000 ("IT Act"), enacted to give legal recognition to electronic commerce and subsequently amended in 2008 to introduce a wider array of substantive cyber-offences, intermediary liability provisions and investigative powers. For over two decades, the IT Act operated alongside the Indian Penal Code, 1860 ("IPC"), the Code of Criminal Procedure, 1973 ("CrPC") and the Indian Evidence Act, 1872 ("IEA"), which supplied the general criminal-law and procedural scaffolding within which cyber-offences were investigated and prosecuted.

With effect from 1 July 2024, the IPC, CrPC and IEA stand repealed and replaced respectively by the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the

ISSN: 2582-6433

Bharatiya Sakshya Adhiniyam, 2023[1]. This is the most substantial overhaul of India's general criminal law since Independence, and it directly affects the investigation, evidentiary treatment and prosecution of cyber-offences, since the BNS incorporates several cyber-related offences within its general scheme (rather than as a distinct chapter), the BNSS revises the procedure governing search, seizure and forensic examination of electronic devices, and the BSA substantially recasts the law relating to the admissibility of electronic records through Sections 61 and 63, replacing the celebrated and much-litigated Section 65B of the IEA.

This paper is animated by a simple but under-examined question: has the transition to the new criminal-law trio strengthened, weakened, or left substantially unaltered the effectiveness of cybercrime investigation in India, when read together with the IT Act? The inquiry is significant because cyber-offences are rarely prosecuted under the IT Act alone; in practice, the police routinely invoke overlapping provisions of the IT Act and the general penal code (now the BNS) in the same First Information Report, producing a dual, and at times inconsistent, framework of offence definitions, sentencing and procedural safeguards.

1.1 Statement of the Problem

Despite two decades of legislative amendment and institutional expansion, India's cybercrime investigation and prosecution ecosystem continues to be marked by strikingly low conviction rates, chronic shortages of trained cyber-forensic examiners at the district level, jurisdictional uncertainty in cross-border offences, and delays in obtaining electronic evidence from foreign intermediaries. The enactment of the BNS, BNSS and BSA presented a legislative opportunity to consolidate and modernise this framework; whether that opportunity has been substantively realised, or whether the new laws largely reproduce the structural weaknesses of their predecessors, is the central problem this paper investigates.

1.2 Research Objectives

- To trace the evolution of substantive and procedural cyber-offence law in India from the IT Act, 2000 to the BNS, BNSS and BSA, 2023.
- To critically examine the investigative powers, search-and-seizure procedure, and digital-forensic safeguards available to law-enforcement agencies under the amended

[1]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023); The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023); The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023); all three statutes were brought into force with effect from 1 July 2024 vide notifications issued by the Ministry of Home Affairs.

ISSN: 2582-6433

framework.

- To analyse the treatment of electronic evidence under Section 63 of the BSA in light of the Supreme Court's jurisprudence on Section 65B of the IEA.
- To evaluate the institutional architecture — CERT-In, the Indian Cyber Crime Coordination Centre (I4C), State Cyber Cells and the National Cyber Crime Reporting Portal — against contemporary cybercrime typologies.
- To identify persistent doctrinal and institutional gaps and to propose reform-oriented recommendations.

1.3 Research Questions

- Does the co-existence of the IT Act and the BNS create harmful overlap, redundancy or sentencing disparity in the prosecution of cyber-offences?
- Do the amended search-and-seizure provisions under the BNSS adequately safeguard the integrity of digital evidence during investigation?
- Has Section 63 of the BSA resolved the doctrinal uncertainty that surrounded Section 65B of the IEA, or has it merely relocated the difficulty?
- Are India's institutional and international-cooperation mechanisms adequate to address the transnational character of contemporary cyber-fraud?

1.4 Research Methodology

This paper adopts a doctrinal, black-letter method of legal research, supplemented by analytical and comparative techniques. Primary sources consist of the text of the IT Act, 2000, the BNS, BNSS and BSA, 2023, subordinate legislation (including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and the CERT-In Directions of 2022), and reported judicial decisions of the Supreme Court and High Courts. Secondary sources include peer-reviewed journal articles, government and parliamentary reports, and official statistical data released by the Ministry of Home Affairs and the National Crime Records Bureau. The paper is structured around a qualitative doctrinal analysis rather than empirical field data, and its findings are accordingly interpretive rather than statistically generalisable.

2. LITERATURE REVIEW

Scholarship on cybercrime and Indian law can be organised into three broad strands: (i) commentary on the substantive and procedural architecture of the IT Act, 2000; (ii)

ISSN: 2582-6433

jurisprudential analysis of electronic evidence, principally centred on Section 65B of the erstwhile Evidence Act; and (iii) an emerging body of literature, largely produced after July 2024, examining the cyber-related provisions of the BNS, BNSS and BSA.

Early commentary on the IT Act, including the widely cited work of Duggal on Indian cyber law, emphasised the statute's origins in the UNCITRAL Model Law on Electronic Commerce and its consequent orientation toward validating electronic transactions rather than comprehensively criminalising cyber-harms. Sharma's treatment of information technology law similarly observed that the 2008 amendment — enacted in the aftermath of the 26/11 Mumbai attacks — expanded the substantive offence provisions (Sections 66A to 66F, 67 to 67C) but simultaneously introduced Section 66A, whose vague and overbroad wording targeting "grossly offensive" online speech was ultimately struck down by the Supreme Court as unconstitutional.

Fatima's work on cybercrimes situates the IT Act within a broader critique of India's fragmented approach: because the IT Act was not designed as an exhaustive penal code, investigators and prosecutors have consistently had to invoke the general penal code in tandem with IT Act provisions, producing charge-sheets that combine, for instance, Section 66C of the IT Act (identity theft) with the offence of cheating under the general penal law[2]. This structural duality is a recurring theme in the literature and forms a central analytical thread of the present paper.

A second, substantial strand of scholarship addresses the admissibility of electronic evidence. The Supreme Court's decision in Anvar P.V. v. P.K. Basheer clarified that a certificate under Section 65B(4) of the IEA was mandatory for the admission of computer-generated evidence, overruling earlier precedent that had permitted proof by oral testimony alone. This position was affirmed and elaborated by a three-judge bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, which held that the certificate requirement could not be dispensed with even where the device in question was not in the possession of the party seeking to rely upon it, subject to the party being permitted to secure the requisite certificate through an application to the court. Commentary on this line of authority — much of it produced in law-review

[2]Talat Fatima, Cybercrimes (2nd edn, Eastern Book Company 2016); see also Pavan Duggal, Cyberlaw: The Indian Perspective (6th edn, Saakshar Law Publications 2021); Vakul Sharma, Information Technology: Law and Practice (5th edn, Universal Law Publishing 2018).

ISSN: 2582-6433

symposia between 2015 and 2023 — consistently identified the certificate requirement as a source of investigative delay and evidentiary loss, particularly in prosecutions dependent on WhatsApp chats, call detail records and CCTV footage held by third parties.

The third and most recent strand of literature responds directly to the 2023 legislative overhaul. Naik's critical examination of the BNS observes that the new code, notwithstanding its stated objective of modernisation, does not create a discrete chapter for cybercrime, choosing instead to graft digital modalities onto pre-existing offence categories such as cheating, forgery, criminal intimidation and organised crime. Similarly, K.S.'s integrated study of the Bharatiya Nyaya (Second) Sanhita, 2023 in the Jus Corpus Law Journal argues that while the substitution of Section 63 of the BSA for Section 65B of the IEA introduces a clearer dual-certification mechanism, it does not fully resolve the doctrinal tension identified in Arjun Panditrao Khotkar, and indeed introduces new interpretive questions concerning the relationship between the newly inserted Section 61 (which purports to permit proof of electronic records by any method otherwise permissible) and Section 63. Recent case commentary — including analysis of the Kerala High Court's 2025 decision in Alukas Jewellery v. Anil, which characterised the absence of a Section 63 certificate as a curable defect rather than a bar to admissibility — suggests that courts are, in effect, continuing the flexible, purposive interpretation developed under the earlier evidentiary regime.

A parallel body of policy literature, produced by the Ministry of Home Affairs, the Parliamentary Standing Committee on Home Affairs (in its 254th Report on the alarming rise in cybercrime and its ramifications), and non-governmental research bodies such as CyberPeace, has documented the institutional response to the crisis, including the establishment of the Indian Cyber Crime Coordination Centre (I4C) in 2020, the Citizen Financial Cyber Fraud Reporting and Management System, and, more recently, the national registry of suspected cybercriminal identifiers launched in coordination with banks. These reports consistently identify capacity constraints — the shortage of trained cyber-forensic examiners, inadequate district-level cyber cells, and low FIR-to-conviction ratios — as the primary bottleneck limiting the effectiveness of an otherwise expanding legal and institutional apparatus. This paper builds on and synthesises these three strands, offering an integrated doctrinal assessment of the substantive, procedural and institutional dimensions of cybercrime investigation across the pre- and post-2024 legal regimes.

ISSN: 2582-6433

3. ANALYSIS AND DISCUSSION

3.1 The Substantive Architecture of the Information Technology Act, 2000

The IT Act was originally enacted to accord legal recognition to electronic records and digital signatures, in fulfilment of India's obligations under the UNCITRAL Model Law on Electronic Commerce, 1996[3]. Its penal architecture was substantially expanded by the Information Technology (Amendment) Act, 2008, which inserted a wide array of cyber-offences: Section 43 (civil liability for unauthorised access, data theft and the introduction of computer contaminants), Section 66 (criminalising the acts described in Section 43 where committed dishonestly or fraudulently), Section 66B (receiving stolen computer resources), Section 66C (identity theft), Section 66D (cheating by personation using a computer resource), Section 66E (violation of privacy), and Section 66F (cyber terrorism). Sections 67, 67A and 67B separately criminalise the publication and transmission of obscene, sexually explicit, and child sexual abuse material in electronic form.

The IT Act's investigative provisions are principally located in Section 78, which empowers a police officer not below the rank of Inspector to investigate offences under the Act, and Sections 69, 69A and 69B, which confer powers of interception, blocking and monitoring on the Central Government subject to procedural safeguards. Section 79 establishes a conditional "safe harbour" for intermediaries, the contours of which were significantly narrowed by the Supreme Court in Shreya Singhal v. Union of India[4], which read down the phrase "actual knowledge" in Section 79(3)(b) to require a court order or government notification, rather than a mere private complaint, before an intermediary could be compelled to take down content. The same judgment struck down Section 66A of the IT Act in its entirety, holding that its criminalisation of "grossly offensive" and "menacing" online communication was unconstitutionally vague and had a chilling effect on protected speech under Article 19(1)(a) of the Constitution. Despite this unambiguous holding, subsequent research by civil-society organisations documented continued — and unlawful — registration of FIRs under the struck-down provision for several years thereafter, a fact that the Supreme Court found necessary to specifically deprecate in a further round of contempt proceedings, underscoring a persistent gap between doctrinal pronouncement and police-station-level practice.

Two early trial-court decisions remain instructive on the practical difficulties of cybercrime investigation under the original IT Act framework. In State of Tamil Nadu v. Suhas Katti, decided in 2004, the accused was convicted under Section 469 IPC (forgery for the purpose of

[3]The Information Technology Act, 2000 (Act 21 of 2000), Preamble.
[4]Shreya Singhal v. Union of India, (2015) 5 SCC 1.

ISSN: 2582-6433

harming reputation) and Section 67 of the IT Act for posting obscene and defamatory messages about the complainant in a Yahoo message group; the case is frequently cited as India's first cybercrime conviction and illustrates the early reliance on IPC provisions to supplement the IT Act's comparatively narrow substantive scope. In Avnish Bajaj v. State (NCT of Delhi), arising from the sale of an obscene video clip through the Baazee.com auction platform, the Delhi High Court considered the criminal liability of the website's Managing Director and clarified the scope of intermediary liability under Section 85 of the IT Act — an issue that would only be comprehensively resolved a decade later in Shreya Singhal.

3.2 Cyber-Offences under the Bharatiya Nyaya Sanhita, 2023

The BNS does not create a self-contained chapter on cybercrime; instead, following the drafting philosophy of the IPC that it replaces, it embeds digital modalities within pre-existing offence categories. This design choice has attracted both defence and criticism in the literature. Its defenders argue that cybercrime is, in substance, traditional criminal conduct — theft, cheating, forgery, intimidation, defamation, stalking and voyeurism — merely committed through a new instrumentality, and that a separate cyber-chapter would risk artificial and under-inclusive categorisation. Its critics respond that the absence of a consolidated cyber-chapter perpetuates the very duplication with the IT Act that has long complicated charge-framing and sentencing consistency.

Several BNS provisions are of particular relevance. Section 111 introduces, for the first time in general criminal law (as opposed to state-specific organised-crime statutes), a consolidated offence of "organised crime", the definition of which expressly includes cyber-crime as a predicate offence where committed by a crime syndicate for pecuniary gain[5]. This is a significant development given the well-documented involvement of organised, often cross-border, syndicates in investment-fraud and "digital arrest" scams. Section 316 (criminal breach of trust) and Section 318 (cheating) retain the structure of their IPC predecessors (Sections 405 and 420) but are routinely invoked alongside Section 66D of the IT Act in online-fraud prosecutions. Section 319, dealing with cheating by personation, expressly contemplates impersonation through electronic means, an improvement in textual clarity over Section 419 IPC. Section 336, governing forgery, expressly extends to the forgery of electronic records, consolidating what had previously required a combined reading of Sections 463, 465 and 29A of the IPC.

[5]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 111(1).

ISSN: 2582-6433

The provisions on stalking, voyeurism and outraging modesty (Sections 78, 77 and 79 BNS, corresponding to Sections 354D, 354C and 354A IPC) similarly retain express references to monitoring a woman's use of the internet, e-mail and electronic communication, and to capturing or transmitting images of a private act without consent[6], provisions that have gained heightened importance amid the rise of non-consensual intimate-image sharing and deepfake pornography. Sections 351 and 356, dealing with criminal intimidation and defamation, continue to be interpreted by courts as extending to electronic communication, sustaining the jurisprudential continuity established under the corresponding IPC provisions in the context of cyberstalking and online extortion, including the increasingly prevalent "digital arrest" modality of extortion, in which fraudsters impersonate law-enforcement or judicial officers over video calls.

3.3 Investigative Procedure under the Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS introduces several procedural innovations of direct relevance to cybercrime investigation. Section 105 mandates audio-video recording of the search and seizure process, including of electronic devices, a safeguard intended to reduce disputes over the integrity of the chain of custody — a recurring evidentiary weakness identified in prior cybercrime prosecutions[7]. Section 173 expressly codifies the practice of Zero FIR (registration of a cognizable offence irrespective of territorial jurisdiction, with subsequent transfer to the competent police station) and permits registration of information relating to a cognizable offence through electronic communication, a provision of considerable practical significance for cybercrime victims, who are frequently unable to identify the situs of the offence given the inherently borderless character of online fraud.

The BNSS also revises timelines for the filing of the police report (charge-sheet) and introduces provisions for the use of forensic science expertise in offences punishable with seven years' imprisonment or more, mandating that a forensic expert visit the crime scene to collect evidence in such cases. Given that several cyber-offences — including cyber terrorism under Section 66F of the IT Act and organised cyber-fraud under Section 111 of the BNS — attract sentences exceeding this threshold, the provision creates, at least in principle, a statutory expectation of forensic rigour that was previously a matter of departmental practice rather than binding law. Whether India's district-level forensic infrastructure possesses the capacity to satisfy this obligation on a nationwide scale is, however, a separate and largely unresolved

[6]The Bharatiya Nyaya Sanhita, 2023, ss. 77-79.
[7]The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s. 105.

ISSN: 2582-6433

institutional question, addressed further in Section 3.7 below.

3.4 Electronic Evidence: From Section 65B of the Evidence Act to Section 63 of the BSA

The admissibility of electronic evidence has historically been the single most litigated procedural issue in Indian cybercrime prosecutions. Section 65B of the erstwhile Indian Evidence Act, 1872 required that secondary evidence of an electronic record — such as a printout of a CCTV recording, a call detail record, or a WhatsApp chat log — be accompanied by a certificate identifying the device on which it was produced and confirming that the device was functioning properly at the relevant time. In State (NCT of Delhi) v. Navjot Sandhu, the Supreme Court initially permitted such evidence to be proved without a certificate, provided there was other corroborating evidence[8]. This position was overruled in Anvar P.V. v. P.K. Basheer, where a three-judge bench held that a Section 65B certificate was a mandatory pre-condition for the admissibility of electronic evidence, and that the earlier permissive approach in Navjot Sandhu did not lay down correct law.

The subsequent decision in Shafhi Mohammad v. State of Himachal Pradesh introduced a further complication by holding that the certificate requirement could be relaxed where the device in question was not in the possession of the party seeking to rely on the evidence[9], creating a period of doctrinal uncertainty that was authoritatively resolved by a three-judge bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, which overruled Shafhi Mohammad and reaffirmed Anvar P.V., while clarifying that a party unable to produce the certificate could apply to the court to direct the production of the certificate by the person in possession of the relevant device.

Section 63 of the BSA now governs this field, replacing Section 65B in near-identical structural terms but introducing a dual-certification requirement: a certificate from the person in charge of the relevant device (setting out particulars of the device, its operating conditions, and the hash value of the electronic record) and, in specified circumstances, an additional certificate from an expert[10], the format of which is now prescribed in a Schedule to the Act — a welcome clarification given that the absence of a prescribed format had itself generated litigation under the earlier regime. Simultaneously, Section 61 of the BSA provides that nothing in the Adhiniyam shall be construed to deny the admissibility of an electronic record merely on the ground that it is an electronic record, and that such a record may be proved in accordance with

[8]State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[9]Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[10]The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63(4) and the Schedule thereto.

ISSN: 2582-6433

the provisions applicable to documents generally

The relationship between Sections 61 and 63 remains doctrinally unsettled. One reading treats Section 61 as confirming that a copy of an electronic record may be proved by any method otherwise available under the Act — including, for example, primary evidence or oral testimony where the original device itself is produced — while Section 63 supplies a special, more convenient mode of proof (the certificate route) that a party may elect to use in lieu of examining a witness. On this reading, Section 61 operates to legislatively supersede the strict, exclusivity-based interpretation of the certificate requirement adopted in Arjun Panditrao Khotkar[11]. Emerging High Court practice appears to support a flexible approach: in Alukas Jewellery v. Anil, decided by the Kerala High Court in July 2025, the absence of a Section 63 certificate was held to be a curable defect going to the mode of proof rather than a bar to admissibility

For cybercrime investigation specifically, this evolving position carries significant practical consequences. Investigating officers seizing digital evidence — server logs from payment gateways, KYC records from banks, call detail records from telecom operators — must now ensure compliance with the Section 63 certification protocol from the point of seizure, since retrospective certification from third-party custodians (particularly foreign-based platforms) remains slow and, in many cases, unobtainable within the statutory investigation period. The introduction of mandatory hash-value recording is a positive development for chain-of-custody integrity, but its practical efficacy depends entirely on the availability of trained personnel and standard operating procedures at the level of the investigating police station — an institutional capacity that, as discussed in Section 3.7, remains uneven across States[12].

3.5 Institutional Architecture: I4C, CERT-In and the National Cyber Crime Reporting Ecosystem

The institutional response to cybercrime has expanded considerably since 2018. The Indian Cyber Crime Coordination Centre (I4C), established under the Ministry of Home Affairs, functions as the principal coordinating body, operating the National Cyber Crime Reporting Portal and the toll-free helpline "1930" for immediate reporting of financial fraud. Since its establishment in its current expanded form in September 2024, I4C has facilitated the sharing

[11]See Saji Koduvath, "Nothing in this Adhiniyam Shall Apply to Deny the Admissibility — New Provision (S. 61, BSA) to Ensure that S. 63, BSA (S. 65B, Evidence Act) is an Enabling Provision" (2025) (analysing the interaction between ss. 61 and 63 BSA in light of Arjun Panditrao Khotkar).

[12]Ministry of Home Affairs, Standard Operating Procedure for Investigation of Cyber Crime Cases, Indian Cyber Crime Coordination Centre (I4C) guidelines.

ISSN: 2582-6433

of over 18.43 lakh suspect identifiers and 24.67 lakh mule bank accounts by partner banks, contributing to the blocking of fraudulent transactions exceeding ₹8,031 crore[13]. The Citizen Financial Cyber Fraud Reporting and Management System, in operation since 2021, has separately been credited with saving over ₹7,130 crore across more than 23 lakh complaints through immediate transaction-freezing mechanisms.

The Indian Computer Emergency Response Team (CERT-In), constituted under Section 70B of the IT Act, functions as the national nodal agency for cybersecurity incident response[14]. Its 2022 Directions mandate that service providers, intermediaries and body corporates report specified categories of cybersecurity incidents within six hours of detection and preserve relevant logs for a minimum of 180 days — a data-retention obligation of direct evidentiary value to investigating agencies, since it partially addresses the perennial problem of critical log data being overwritten or deleted before an investigating officer can secure it. Nonetheless, the six-hour reporting window has drawn criticism from industry bodies as operationally onerous, and compliance across the vast intermediary ecosystem, particularly among smaller platforms, remains inconsistent.

At the State level, investigation is carried out by dedicated Cyber Crime Police Stations and Cyber Cells, whose capacity varies markedly across jurisdictions. States such as Telangana, Maharashtra and Karnataka have developed comparatively well-resourced cyber-forensic laboratories, while several smaller States and Union Territories continue to rely on a limited number of centrally-located forensic facilities, resulting in significant delays in obtaining forensic reports — delays that, given statutory limitation periods for filing charge-sheets under the BNSS, directly threaten the successful prosecution of time-sensitive cyber-offences.

3.6 Statistical Overview and Emerging Typologies (2021–2026)

Quantitative indicators drawn from Ministry of Home Affairs data and parliamentary disclosures illustrate both the scale of the challenge and the partial success of recent institutional interventions. Cybercrime complaints registered on the NCRP rose from 2.62 lakh in 2021 to 9.66 lakh in 2022, 15.56 lakh in 2023, 22.68 lakh in 2024 and 28.15 lakh in 2025 — a more than tenfold increase in five years. Reported financial losses rose from approximately ₹551 crore in 2021 to a peak of approximately ₹22,845 crore in 2024, declining marginally to ₹22,495 crore in 2025, a decline attributed by the Ministry to more effective real-time

[13]Ministry of Home Affairs, reply to Lok Sabha Unstarred Question, December 2025, cited in "Indians Lost Rs 22,495 Crore to Cyber Fraud in 2025, Investment Scams Account for 75%", The Print, 21 February 2026.
[14]The Information Technology Act, 2000, s. 70B.

ISSN: 2582-6433

transaction-blocking rather than to any underlying reduction in fraudulent activity. Notably, while complaint volumes rose sharply, the number of FIRs actually registered fell from 66,370 in 2024 to 55,484 in 2025, a divergence that officials attribute to faster pre-FIR intervention by banks and I4C but which also raises the question, examined further in Section 4 below, of whether a growing proportion of cyber-fraud complaints are being resolved through informal fund-freezing mechanisms rather than through formal criminal investigation and prosecution.

Investment-related scams — including fraudulent trading applications and fake stock-tip schemes — accounted for over 75 per cent of reported financial losses in 2025, followed by "digital arrest" extortion (approximately 8–9 per cent), credit-card and banking fraud (approximately 7 per cent), sextortion (approximately 4 per cent), and e-commerce and malware-based fraud (approximately 4 per cent combined). The prominence of investment fraud and digital-arrest extortion reflects the growing sophistication of organised, often cross-border, criminal networks employing psychological-manipulation techniques rather than purely technical exploits, a shift that has significant implications for investigative methodology, since these offences typically leave a financial and communications trail (bank transfers, call records, video-call metadata) that is more amenable to forensic reconstruction than purely technical intrusions, provided investigating agencies possess the requisite training and inter-agency cooperation mechanisms to trace it.

3.7 Cross-Border Investigation and International Cooperation

A substantial proportion of contemporary cyber-fraud targeting Indian victims originates from criminal syndicates operating outside India's territorial jurisdiction, including from scam compounds in Cambodia, Myanmar and Laos. Investigation of such offences requires resort to mutual legal assistance treaties (MLATs), Letters Rogatory, and cooperation channels with foreign law-enforcement and INTERPOL, processes that remain comparatively slow relative to the short window within which digital evidence — server logs, IP-address allocation records — typically remains available before deletion by the custodian platform.

India has not acceded to the Council of Europe's Budapest Convention on Cybercrime, 2001, historically citing concerns regarding sovereignty and the treaty's negotiation without India's participation. India adopted a similar posture toward the United Nations Convention against Cybercrime, adopted by the UN General Assembly on 24 December 2024 and opened for signature at Hanoi on 25 October 2025[15]: as of the signing ceremony, 72 of 193 UN member

[15]United Nations Convention against Cybercrime, adopted by UN General Assembly Resolution 79/243 (24 December 2024), opened for signature at Hanoi, Viet Nam, 25 October 2025.

ISSN: 2582-6433

States had signed the Convention, but India was not among them, reportedly owing to continuing evaluation of the treaty's implications for data-sharing obligations, sovereignty and domestic privacy safeguards recognised in Justice K.S. Puttaswamy v. Union of India

The UN Convention, which will enter into force ninety days after the fortieth instrument of ratification or accession and remains open for signature until 31 December 2026, is significant for Indian cybercrime investigation because it establishes, for the first time, a near-universal legal framework for the expedited preservation and cross-border sharing of electronic evidence in serious offences. India's continued non-accession — while defensible on sovereignty and privacy grounds — leaves Indian investigating agencies dependent on the comparatively slower bilateral MLAT process for evidence located in non-cooperating or non-treaty jurisdictions, a structural constraint that this paper identifies as one of the most significant unresolved gaps in the post-2024 legal framework, since neither the BNSS nor the BSA meaningfully addresses the cross-border dimension of digital evidence-gathering[16].

3.8 The Data Protection Interface: The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("DPDP Act"), though primarily a data-governance rather than a criminal statute, has an important, if underappreciated, bearing on cybercrime investigation[17]. Section 17(2)(a) of the DPDP Act exempts the processing of personal data for the prevention, detection, investigation or prosecution of offences from several of the Act's general consent and purpose-limitation obligations, thereby preserving investigating agencies' access to data held by regulated data fiduciaries. However, the interaction between this investigative exemption and the DPDP Act's data-localisation and cross-border-transfer provisions has not yet been authoritatively tested in the cybercrime context, and commentators have flagged the risk that data fiduciaries, out of an abundance of caution, may resist voluntary disclosure to investigating officers absent a formal court order — a friction that did not exist, in equivalent form, prior to the DPDP Act's enactment.

3.9 Judicial Interpretation and Jurisdictional Questions

Beyond the evidentiary jurisprudence discussed above, courts have grappled with the territorial scope of the IT Act. Section 75 of the IT Act extends the Act's application to offences committed outside India where the offence involves a computer, computer system or network

[16]K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (recognising the fundamental right to privacy and its implications for state data-collection and cross-border data-sharing practices).
[17]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

ISSN: 2582-6433

located in India, a provision of considerable importance given the transnational character of most contemporary cyber-fraud. Courts have also addressed the boundary between civil copyright/trademark infringement claims and criminal cyber-offence provisions, and — in Gagan Harsh Sharma v. State of Maharashtra — clarified the relationship between Sections 43 and 66 of the IT Act (data theft and unauthorised access) and the corresponding provisions of the IPC/BNS relating to theft and criminal breach of trust, holding that where the special provisions of the IT Act cover the field, resort to the general provisions of the penal code for the same conduct requires careful scrutiny to avoid double punishment for a single wrong[18]. This tension between the specific (IT Act) and the general (now BNS) penal provisions remains, in the assessment of this paper, only partially resolved by the 2023 reforms, since neither the BNS nor its Statement of Objects and Reasons expressly addresses the question of provision-overlap with the IT Act.

Aspect	Old Framework (IPC / CrPC / IEA)	New Framework (BNS / BNSS / BSA)
Cyber fraud / cheating	S. 420 IPC (cheating and dishonestly inducing delivery of property)	S. 318 BNS (cheating), read with S. 316 (criminal breach of trust); electronic modality not separately defined
Cheating by personation (fake profiles/e-mail)	S. 419 IPC	S. 319 BNS — expressly extends to impersonation through electronic means
Forgery of electronic records	S. 465/466 IPC read with S. 29A IPC (electronic record as "document")	S. 336 BNS, expressly covering forged electronic records
Organised cybercrime / cyber-fraud syndicates	No dedicated provision; MCOCA-type state laws invoked selectively	S. 111 BNS — "organised crime" now expressly includes cyber-crime as a scheduled predicate offence
Criminal intimidation / defamation online (sextortion, digital arrest)	S. 503/499 IPC applied to electronic communication by extension	S. 351/356 BNS — retains structure, judicial extension to electronic media continues
Search & seizure of	S. 100, 165 CrPC — general	S. 105 BNSS — mandatory audio-video

[18]Gagan Harsh Sharma v. State of Maharashtra, 2019 SCC OnLine Bom 1287.

ISSN: 2582-6433

digital devices	search provisions, no mandatory audio-video recording	recording of search and seizure, including of electronic devices
Admissibility of electronic evidence	S. 65B IEA — single certificate by person in charge of device (Anvar P.V.; Arjun Panditrao)	S. 63 BSA — dual certification (device custodian + independent expert) with prescribed Schedule format; S. 61 permits alternative modes of proof
Zero FIR / e-FIR	Zero FIR recognised through executive instructions and judicial practice, not express statutory text	S. 173 BNSS expressly codifies Zero FIR and permits registration of FIR through electronic means for cognizable offences

Table 1: Comparative overview of selected cyber-related provisions under the old and new criminal-law frameworks, read alongside the IT Act, 2000, which continues to apply concurrently under both regimes.

4. FINDINGS

The doctrinal analysis undertaken in Section 3 supports the following principal findings regarding the effectiveness of India's cybercrime investigation framework under the combined operation of the IT Act, 2000 and the BNS, BNSS and BSA, 2023.

1. **Persistent statutory overlap:** The BNS, like the IPC before it, does not consolidate cyber-offences into a discrete chapter, with the result that the IT Act and the BNS continue to operate concurrently over substantially overlapping conduct (cheating, forgery, identity theft, criminal intimidation). This produces charge-sheets invoking multiple overlapping provisions, inconsistent sentencing outcomes across similar fact-patterns, and continuing doctrinal uncertainty of the kind identified in Gagan Harsh Sharma regarding the relationship between special and general penal provisions.

2. **Incremental but meaningful procedural modernisation:** The BNSS introduces genuine improvements relevant to cybercrime investigation — mandatory audio-video documentation of search and seizure under Section 105, express statutory recognition of Zero FIR and e-FIR under Section 173, and a forensic-expert mandate for serious

ISSN: 2582-6433

offences — each of which addresses a specific, previously informal, weakness in cybercrime investigative practice.

3. **Relocation rather than resolution of the electronic-evidence controversy:** Section 63 of the BSA reproduces the substantive structure of Section 65B of the IEA, refines the certification format through a prescribed Schedule, and introduces a dual-certification requirement, but the relationship between the new Section 61 and Section 63 remains textually ambiguous and is only beginning to be tested in reported case law such as Alukas Jewellery v. Anil. The underlying practical bottleneck — the capacity of investigating officers and forensic examiners to generate compliant certificates at the point of seizure — is a matter of institutional capacity that legislative reform alone cannot resolve.

4. **Institutional expansion has outpaced, and partly offset, doctrinal reform:** The most measurable improvements in outcomes — the blocking of over ₹8,031 crore in fraudulent transactions through I4C coordination and over ₹7,130 crore through the Citizen Financial Cyber Fraud Reporting and Management System — have arisen primarily from executive and administrative coordination mechanisms (real-time bank-police-I4C data sharing) rather than from the amended criminal-law text itself.

5. **Declining FIR registration amid rising complaint volumes:** The divergence between rising NCRP complaint numbers (28.15 lakh in 2025) and falling FIR registrations (55,484 in 2025, down from 66,370 in 2024) suggests that an increasing proportion of cyber-fraud cases are being resolved through informal fund-freezing rather than formal criminal investigation, raising concerns regarding both offender accountability and the completeness of official cybercrime statistics.

6. **Persistent capacity deficits at the district level:** Cyber-forensic infrastructure and trained personnel remain concentrated in a small number of States and metropolitan forensic laboratories, undermining the practical realisation of the BNSS's forensic-expert mandate and the BSA's certification requirements in smaller towns and rural districts, which now account for a growing share of victimisation given rising rural internet penetration.

ISSN: 2582-6433

7. **Under-addressed cross-border dimension:** Neither the BNSS nor the BSA meaningfully addresses the cross-border character of contemporary cyber-fraud. India's continued non-accession to the Budapest Convention and to the 2025 UN Convention against Cybercrime leaves investigating agencies reliant on comparatively slow bilateral mutual legal assistance mechanisms, creating a structural mismatch between the transnational nature of the crime and the largely domestic orientation of the applicable procedural law.

8. **Emerging technological typologies outpacing statutory language:** AI-generated deepfakes, voice-cloning and "digital arrest" psychological-manipulation extortion are increasingly prevalent but are prosecuted through purposive extension of existing provisions (criminal intimidation, cheating, impersonation) rather than through dedicated statutory language, creating interpretive uncertainty analogous to that which historically surrounded Section 66A prior to Shreya Singhal.

9. **Untested interface with the DPDP Act, 2023:** While Section 17(2)(a) of the DPDP Act preserves investigative access to personal data, the practical interaction between this exemption and data fiduciaries' compliance incentives has not yet been tested in the cybercrime-investigation context and represents an emerging area of legal uncertainty.

5. RECOMMENDATIONS

Based on the findings above, the following reform-oriented recommendations are proposed for legislative, institutional and policy consideration.

1. **Consolidation of cyber-offences:** Parliament should consider a dedicated Cybercrime Code, or, at minimum, a consolidating schedule cross-referencing overlapping BNS and IT Act provisions, to reduce charge-sheet duplication and to standardise sentencing across functionally identical offences currently punishable under both statutes.

2. **Clarification of the Section 61–Section 63 BSA interface:** The Ministry of Law and Justice, or the Law Commission of India, should issue an authoritative clarificatory circular, or Parliament should amend the BSA, to expressly state the precedence and interaction between Sections 61 and 63, in order to pre-empt the kind of decade-long doctrinal uncertainty that surrounded Section 65B of the IEA.

ISSN: 2582-6433

3. **Nationwide expansion of district-level cyber-forensic capacity:** Central funding under schemes such as the Cyber Crime Prevention against Women and Children (CCPWC) scheme should be scaled to ensure that every district possesses, at minimum, a certified digital-forensic first-responder capable of generating a compliant Section 63 BSA certificate at the point of seizure, supported by mobile forensic units for rural and Tier-3 districts.

4. **Statutory timelines for platform and bank cooperation:** Building on the CERT-In six-hour incident-reporting mandate, Parliament should consider statutorily prescribed response timelines for banks and intermediaries to respond to lawful investigative requisitions (KYC data, transaction logs, IP records), with graded penalties for non-compliance, to reduce the evidentiary attrition that currently occurs during the gap between offence and data preservation.

5. **Reassessment of accession to international cybercrime instruments:** The Government should undertake a transparent, time-bound review of the costs and benefits of accession to the UN Convention against Cybercrime (open for signature until 31 December 2026), with particular attention to the adequacy of its human-rights and data-protection safeguards, given that non-accession leaves Indian investigators structurally disadvantaged in obtaining timely cross-border electronic evidence.

6. **Statutory recognition of emerging typologies:** Explicit statutory provisions addressing AI-generated deepfakes, voice-cloning-based impersonation, and "digital arrest" extortion should be considered, whether through amendment to the IT Act or the BNS, to remove reliance on purposive judicial extension of provisions drafted for a pre-generative-AI threat environment.

7. **Transparent cybercrime data publication:** The National Crime Records Bureau and I4C should jointly publish disaggregated data distinguishing complaints resolved through informal fund-freezing from those culminating in FIR registration, charge-sheet filing and conviction, to enable accurate assessment of investigative — as opposed to merely preventive — effectiveness.

ISSN: 2582-6433

8. **Judicial and prosecutorial training:** Continuing legal education programmes for judicial officers and public prosecutors on the BSA's electronic-evidence provisions and on cyber-forensic methodology should be institutionalised through the National Judicial Academy and State Judicial Academies, given the demonstrated historical correlation between judicial unfamiliarity with electronic evidence and prosecutorial failure.

9. **Harmonising the DPDP Act investigative exemption:** Subordinate legislation or rules under the DPDP Act should clarify the procedural mechanism by which investigating agencies invoke the Section 17(2)(a) exemption, to prevent data fiduciaries from adopting unduly conservative disclosure postures that could delay time-sensitive cybercrime investigations.

6. CONCLUSION

This paper set out to evaluate whether the transition from the IPC, CrPC and IEA to the BNS, BNSS and BSA has strengthened the effectiveness of cybercrime investigation in India when read alongside the IT Act, 2000. The analysis suggests a qualified and differentiated answer. On the procedural plane, the reforms are genuinely significant: the mandatory audio-video documentation of search and seizure, the express statutory recognition of Zero FIR and electronic FIR registration, and the refined dual-certification regime for electronic evidence under Section 63 of the BSA each respond directly to specific, previously informal or judicially improvised, weaknesses in cybercrime investigative practice. These are not cosmetic changes; they represent a considered legislative attempt to modernise procedure for a digital-evidence-dominated criminal-justice environment.

On the substantive and institutional planes, however, the reforms are considerably less transformative. The BNS reproduces, rather than resolves, the structural duplication between general penal law and the IT Act's specialised cyber-offence provisions, leaving investigators and prosecutors to navigate overlapping charge options with limited statutory guidance on sentencing consistency. The most measurable operational improvements of the past three years — the blocking of thousands of crores of rupees in fraudulent transactions — have flowed predominantly from administrative and inter-agency coordination mechanisms such as the I4C's mule-account registry, rather than from the amended criminal-law text itself, suggesting that institutional capacity and inter-agency data-sharing, not statutory drafting, remain the

ISSN: 2582-6433

binding constraint on investigative effectiveness. Meanwhile, the transnational character of contemporary cyber-fraud, increasingly dominated by organised syndicates operating from outside India's territorial jurisdiction, is barely addressed by either the BNSS or the BSA, and India's continued non-accession to prevailing international cybercrime instruments leaves a structural gap that domestic procedural reform, however well-designed, cannot by itself close.

REFERENCES

A. Statutes

1. *The Information Technology Act, 2000 (Act 21 of 2000).*
2. *The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).*
3. *The Indian Penal Code, 1860 (Act 45 of 1860) [repealed].*
4. *The Code of Criminal Procedure, 1973 (Act 2 of 1974) [repealed].*
5. *The Indian Evidence Act, 1872 (Act 1 of 1872) [repealed].*
6. *The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).*
7. *The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).*
8. *The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).*
9. *The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).*
10. *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023.*
11. *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, No. 20(3)/2022-CERT-In, dated 28 April 2022.*
12. *United Nations Convention against Cybercrime, adopted by UN General Assembly Resolution 79/243 (24 December 2024), opened for signature at Hanoi, Viet Nam, 25 October 2025.*
13. *Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185 (23 November 2001).*

B. Cases

14. *Alukas Jewellery v. Anil, Kerala High Court, decided 17 July 2025.*
15. *Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.*
16. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.*
17. *Avnish Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427.*

ISSN: 2582-6433

18. *Gagan Harsh Sharma v. State of Maharashtra, 2019 SCC OnLine Bom 1287.*
19. *Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*
20. *Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.*
21. *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*
22. *State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.*
23. *State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004, Addl. Chief Metropolitan Magistrate, Egmore, Chennai (decided 5 November 2004).*

C. Books

24. *Pavan Duggal, Cyberlaw: The Indian Perspective (6th edn, Saakshar Law Publications 2021).*
25. *Talat Fatima, Cybercrimes (2nd edn, Eastern Book Company 2016).*
26. *Vakul Sharma, Information Technology: Law and Practice (5th edn, Universal Law Publishing 2018).*

D. Journal Articles

27. *A.K. K.S., "The Bhartiya Nyaya (Second) Sanhita 2023: An Integrated Perspective — A Comprehensive Study and Analysis" (2024) Jus Corpus Law Journal 350.*
28. *Y. Naik, "The Bharatiya Nyaya Sanhita (BNS): A Critical Examination of India's New Penal Code" (2024) SSRN Electronic Journal 1.*
29. *Saji Koduvath, "Nothing in this Adhiniyam Shall Apply to Deny the Admissibility — New Provision (S. 61, BSA) to Ensure that S. 63, BSA (S. 65B, Evidence Act) is an Enabling Provision", Indian Law Live (2025).*
30. *Author(s), "Bhartiya Nyay Sanhita and Cyber Crime" (2024) South India Journal of Social Sciences.*
31. *Author(s), "Re-conceptualizing Section 63 of Bharatiya Sakshya Adhiniyam: Judicial Approach to Electronic Evidence in the Age of AI-Generated Content" (2025) 2(4) Career Point International Journal of Research 237.*

E. Reports and Official Sources

32. *Ministry of Home Affairs, Government of India, replies to Lok Sabha Unstarred Questions on cybercrime statistics (2025-2026).*
33. *Parliamentary Standing Committee on Home Affairs, 254th Report on "Alarming Rise in Cyber Crime and Effective Mechanism to Deal with it", Rajya Sabha Secretariat.*

ISSN: 2582-6433

34. *Indian Cyber Crime Coordination Centre (I4C), Standard Operating Procedure for Investigation of Cyber Crime Cases and Annual Statistics, National Crime Records Bureau / Ministry of Home Affairs.*
35. *National Crime Records Bureau, Crime in India (annual reports, various years).*
36. *CyberPeace Foundation, "The Data Behind India's Digital Fraud Surge" (2026).*

F. News and Web Sources (accessed August 2026)

37. *"Cybercrime in India 2025: 24% Spike, ₹22,495 Crore Lost", Insights on India (21 February 2026).*
38. *"Indians Lost Rs 22,495 Crore to Cyber Fraud in 2025, Investment Scams Account for 75%", The Print (21 February 2026).*
39. *"Top 10 Most Highlighted Cyber Crime Cases and Trends in India in 2025", The420.in (27 December 2025).*
40. *"UN Cybercrime Treaty Signed by 72 Nations, India Abstains", MediaNama (28 October 2025).*
41. *United Nations Office on Drugs and Crime, "United Nations Convention against Cybercrime" (unodc.org, accessed August 2026).*