Int. J. Sci. R. Tech., 2026 3(8)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

Cybercrime Investigation in India after the 2023 Criminal-Law Reforms: Integrating Criminal Liability, Digital Evidence, Forensics and Institutional Enforcement

Lathika Karikalan K. M.*, Suresh Kumar R.

The Central Law College, Salem, The Tamil Nadu Dr. Ambedkar Law University

ABSTRACT

Cybercrime investigation in India has entered a new legal phase following the commencement of the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA). These enactments operate alongside the Information Technology Act 2000, the Digital Personal Data Protection Act 2023 (DPDP Act), sectoral regulation and specialised cybercrime institutions. This article argues that the principal weakness of the present framework is not a lack of offences, but fragmentation across legal classification, investigative procedure, digital-evidence rules, forensic practice, privacy governance and institutional coordination. Using doctrinal legal research supplemented by official policy and institutional material, the article develops an investigation-chain framework linking complaint triage, offence classification, preservation, lawful acquisition, forensic examination, attribution, financial tracing, cross-border evidence, prosecution and adjudication. It evaluates the continuing interaction between general criminal liability under the BNS and technology-specific provisions of the Information Technology Act, while examining the evidentiary significance of electronic records under the BSA. Particular attention is given to cloud evidence, cryptocurrency, ransomware, artificial intelligence and deepfakes. The article contends that technological traceability must not be equated with human attribution and that evidentiary reliability depends on the entire acquisition-to-trial chain. It proposes harmonised investigative protocols, accredited forensic capacity, specialist prosecution and judicial training, auditable access to personal data, improved cross-border preservation mechanisms, and a human-verification requirement for significant AI-assisted investigative outputs. The analysis contributes an India-specific but internationally relevant model for assessing whether contemporary cybercrime law can produce reliable, rights-compliant and trial-ready investigations.

Keywords: cybercrime; digital evidence; cyber forensics; privacy; artificial intelligence; cryptocurrency; India.

INTRODUCTION

Digitalisation has changed both the commission of crime and the conditions under which crime must be investigated. A single online fraud can generate evidence across a victim's device, a social-media account, a bank account, a telecommunications network, a cloud service and an exchange located in another jurisdiction. Evidence may be volatile, encrypted, distributed across providers or capable of remote alteration. The investigative problem is consequently not exhausted by identifying the correct criminal offence. It also requires a lawful and technically defensible pathway for preservation, acquisition, authentication, analysis, attribution and presentation at trial.

India's contemporary criminal-law architecture became operational on 1 July 2024. The BNS, BNSS and BSA now provide the general substantive, procedural and evidentiary framework, while the Information Technology Act continues to perform a specialised role in relation to computer-related conduct, electronic systems and intermediary regulation. The DPDP framework adds a distinct data-governance dimension. The supplied manuscript correctly identifies this system as a legal ecosystem rather than a single cybercrime statute. [1-5]

The article's central proposition is that cybercrime enforcement should be evaluated as an investigation-to-adjudication chain. A legally available offence is of limited practical value if evidence cannot be preserved in time; a technically authentic record is of

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

limited value if its provenance cannot be established; and an investigative power is of limited legitimacy if its exercise is disproportionate or insufficiently auditable. The article therefore shifts the analytical focus from statutory enumeration to interoperability.

The contribution is fourfold. First, it maps the interaction between the BNS, BNSS, BSA and Information Technology Act according to investigative stage. Second, it separates technical integrity from attribution and explains why both must be proved through cumulative evidence. Third, it connects digital forensics, privacy and institutional coordination rather than treating them as separate subjects. Fourth, it develops reform proposals that are capable of application beyond India, particularly in jurisdictions confronting similar problems of cloud evidence, synthetic media, cryptocurrency and cross-border investigations.

2. LITERATURE AND RESEARCH GAP

Indian cybercrime scholarship has developed around several established strands: the Information Technology Act and technology-specific offences; electronic evidence and the former Section 65B regime; privacy and surveillance; intermediary liability; and emerging risks such as ransomware, cryptocurrency fraud, deepfakes and artificial intelligence. Judicial decisions including Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal remain important to understanding the evidentiary transition from the Indian Evidence Act to the BSA. [6-7]

The limitation of a statute-by-statute approach is operational. A contemporary cyber investigation rarely belongs to one statute. A phishing incident may require BNS liability, Information Technology Act provisions, BNSS investigative procedure, BSA proof of electronic records, banking intervention, platform disclosure and privacy-sensitive handling of personal information. Existing discussions therefore need to be complemented by a framework that explains how these legal components interact sequentially.

The research gap is especially significant after the 2023 enactments. The transition to the BSA requires renewed attention to provenance, authenticity, integrity, computer output and the relationship between admissibility and evidentiary weight. Similarly, the BNSS must be evaluated not merely for electronic procedural facilities but for how those facilities interact with search, seizure, preservation, forensic acquisition and judicial oversight. The present study addresses this gap through an investigation-chain model.

3. Research Questions, Objectives and Hypothesis

The study asks: (1) whether the BNS, BNSS and BSA provide a coherent framework for contemporary cybercrime investigation; (2) how BNS offences should be distinguished from technology-specific offences under the Information Technology Act; (3) whether the BSA adequately supports authenticity, integrity and admissibility of electronic evidence; (4) how investigators can access digital and personal data consistently with legality, necessity and proportionality; and (5) whether current mechanisms are adequate for AI-enabled crime, deepfakes, cryptocurrency, cloud evidence and transnational investigations.

The objectives are to analyse the relevant criminal liability, procedural and evidentiary provisions; evaluate the continuing role of the Information Technology Act; examine the privacy dimension of investigative access; develop an investigation-chain model; assess forensic and emerging-technology challenges; evaluate institutional interoperability; and propose legally defensible reforms.

Hypothesis: India's cybercrime framework is substantively broad but operationally fragmented. Investigation outcomes therefore depend less on adding offences than on procedural harmonisation, forensic reliability, institutional coordination, timely financial intervention and constitutionally compliant access to digital evidence.

4. METHODOLOGY AND ANALYTICAL FRAMEWORK

This is a doctrinal legal study supplemented by policy and official institutional material. Primary sources include the Constitution of India, the BNS, BNSS, BSA, Information Technology Act, DPDP Act and subordinate instruments. Judicial authorities are used to test propositions concerning electronic evidence, privacy, technology-mediated testimony and the relationship between general criminal law and

technology-specific regulation. Secondary materials comprise scholarly literature, law reviews, books and institutional publications.

The analytical method is functional rather than merely descriptive. Each legal instrument is assessed according to the stage at which it becomes relevant: classification, preservation, acquisition, forensic analysis, attribution, financial tracing, cross-border evidence, prosecution and adjudication. This approach avoids treating statutes as self-contained compartments.

Official statistics are not collapsed into a single measure of cybercrime. NCRB registered-crime data, National Cyber Crime Reporting Portal complaints, CFCFRMS intervention figures and CERT-In incident data measure different phenomena. They should therefore be cited with their respective definitions, dates and institutional provenance. The article does not infer prevalence or conviction performance from one dataset alone.

5. Criminal Liability under the BNS and the Continuing Role of the Information Technology Act

The BNS is not a specialised cybercrime code. Its significance is that many digitally facilitated offences remain legally intelligible through general criminal concepts. Online deception may constitute cheating; fraudulent impersonation may engage provisions concerning personation; manipulated records may raise forgery issues; online threats may amount to criminal intimidation; and coordinated digital conduct may engage conspiracy or organised-crime concepts where statutory elements are satisfied. The technological medium should not obscure the elements of the offence.

At the same time, technology-specific conduct may fall within the Information Technology Act. The Act remains relevant to specified unauthorised computer-related acts, electronic content, interception or decryption mechanisms, protected systems and intermediary safe harbour. Section 66A is not a live offence: Shreya Singhal v. Union of India struck it down, demonstrating that cyber enforcement remains subject to constitutional limits on vague restrictions of speech. [8]

The practical implication is complementary charging. Where conduct potentially engages both general criminal law and the Information Technology Act, investigators and prosecutors should identify the factual conduct, the distinct statutory ingredients and the evidence supporting each ingredient. Overlap should not become a substitute for precise legal classification.

6. BNSS and the Investigation of Digital Crime

The BNSS provides the procedural environment within which cybercrime investigation takes place. Its importance lies less in creating an isolated cyber procedure than in accommodating contemporary electronic processes within criminal procedure. Digital notices, records and proceedings can improve efficiency, but technological convenience cannot displace legality, fairness or judicial supervision.

A defensible investigation can be represented as a sequence: complaint and triage; legal classification; immediate preservation; identification of devices, accounts and providers; lawful acquisition; forensic imaging and integrity verification; analysis and attribution; financial tracing; cross-border preservation or disclosure; and prosecution supported by a coherent evidentiary narrative.

Search and seizure are particularly sensitive because a single device can contain communications, financial records, photographs, credentials and unrelated personal information. Investigators should document device condition, acquisition method, examiner identity, hash values, storage media and every material transfer. Where live acquisition is necessary because volatile memory, active encryption or running processes may be material, the decision and methodology should be documented.

The investigation diary and forensic record should permit a court to reconstruct what was obtained, by whom, when, through which method and with what limitations. The goal is not maximal collection; it is reliable and legally authorised collection of material that can be connected to the alleged offence.

7. BSA and the Reliability of Digital Evidence

The BSA expressly incorporates electronic and digital records into the evidence framework. Section 61

recognises electronic or digital records, while Section 63 addresses admissibility requirements concerning electronic records and computer output. The transition from the former Section 65B regime should not be understood as automatic acceptance of every electronic artefact. The continuing concern is reliability.

Three questions should be kept analytically distinct: admissibility, authenticity and evidentiary weight. A screenshot may be relevant but weakly probative if provenance, authorship or integrity is uncertain. Conversely, properly acquired forensic images, provider records and corroborated server logs may provide stronger evidence. The court's task is therefore not simply to ask whether information is digital, but whether the evidentiary chain makes the proposed inference reliable.

The Supreme Court's electronic-evidence jurisprudence remains relevant to this logic. Anvar P.V. established the importance of the statutory approach to electronic records; Arjun Panditrao clarified the certificate requirement under the former law; Tomaso Bruno emphasised the value of scientific and electronic evidence; and State of Maharashtra v. Dr. Praful B. Desai recognised video-conferencing as a permissible means of taking evidence where fairness is maintained. [6,7,9,10]

Digital evidence should ordinarily be corroborated across sources. Messages may be tested against device artefacts, provider records and metadata; emails against headers and server information; and cryptocurrency transactions against blockchain records, exchange information and lawful KYC material. Technical traceability is evidence of a connection, not automatically proof of human responsibility.

8. Digital Forensics, Integrity and Attribution

Digital forensics is the methodological bridge between technological artefacts and courtroom evidence. A defensible process includes identification, preservation, acquisition, examination, analysis, interpretation and reporting. The forensic record should identify the device condition, examiner, tools and versions used, acquisition method, hash values, relevant timestamps and material analytical steps.

Hashing is an integrity mechanism. It can demonstrate that a forensic image or extracted dataset corresponds to the material acquired earlier, but it does not prove who created a file, controlled an account or committed an offence. Attribution must therefore be constructed cumulatively from device possession, authentication records, subscriber information, transaction history, communications, access records and other lawfully obtained artefacts.

Cloud and mobile forensics complicate the chain because encryption, synchronisation, remote wiping and provider architecture can alter the investigative environment. Evidence may also be stored outside India. Preservation requests and lawful provider disclosure should therefore be considered early rather than after local evidence has been exhausted.

Expert reports should state the finding, method, integrity checks, inference supported, alternative explanations and limitations. Transparent limitations enhance judicial reliability because they allow the court to distinguish observation from interpretation.

9. Privacy, Data Governance and Constitutional Limits

Cyber investigations routinely involve personal data obtained from devices, banks, telecommunications providers, platforms and cloud services. Data governance is therefore part of criminal procedure rather than an external policy concern. Investigative access should have a legal basis, a defined purpose and safeguards proportionate to the intrusion.

Digital searches can reveal a comprehensive picture of a person's life. The privacy jurisprudence associated with Justice K.S. Puttaswamy (Retd.) v. Union of India therefore provides a constitutional foundation for necessity, proportionality and safeguards in intrusive investigation. [11] The relevant question is not whether privacy and investigation are inherently incompatible, but whether investigative access is legally authorised, necessary, proportionate, secure and reviewable.

The DPDP framework adds an important governance dimension. The article does not treat data protection as an absolute bar to lawful investigation; instead, it argues for minimisation, role-based access, audit trails, purpose limitation, retention controls and

secure handling of irrelevant information. These safeguards can strengthen both privacy and evidentiary reliability.

10. Emerging Technologies and Evidentiary Risk

10.1 Artificial intelligence

AI can facilitate phishing, synthetic content, automated targeting and malware-related activity, while investigators may use machine-assisted detection, clustering and prioritisation. The principal legal risk is overreliance on algorithmic outputs. An AI-generated lead should ordinarily be treated as an investigative lead requiring human verification and independent corroboration, not as proof of guilt.

10.2 Deepfakes

Synthetic audio and video complicate authenticity, provenance and attribution. Examination may consider source history, metadata, compression patterns, frame or audio inconsistencies and provenance information, but no single forensic indicator should be regarded as infallible. Criminal liability must still be connected to the elements of an established offence.

10.3 Cryptocurrency and blockchain

A public blockchain can demonstrate movement between addresses, but it does not necessarily identify the natural person controlling an address. Attribution requires correlation with exchange records, lawful KYC information, device evidence, communications and other investigative material. Investigators should distinguish transaction evidence from ownership or control evidence.

10.4 Ransomware and cloud crime

Ransomware investigations require preservation of ransom notes, malware samples, logs, backups, affected-system artefacts and payment information. Cloud investigations require coordinated preservation and disclosure across affected organisations, providers and investigators. In both settings, the speed of preservation can be as important as the later forensic examination.

11. Institutional Coordination and the Investigation Chain

The institutional architecture includes state police and cyber cells, NCRB, I4C, CERT-In, financial institutions, telecommunications providers, online platforms, forensic laboratories, prosecutors and courts. The presence of these institutions does not itself establish an effective system. Performance depends on interoperability, response time, standard terminology, secure data exchange and the conversion of technical findings into legally usable evidence.

The investigation-chain model proposed here can be stated as follows: Incident → Triage → Legal classification → Preservation → Lawful acquisition → Forensic validation → Attribution → Financial/cross-border tracing → Evidentiary synthesis → Prosecution → Adjudication. Each transition creates a potential failure point. A failure in preservation may make later forensic expertise irrelevant; weak attribution may leave technically authentic evidence disconnected from the accused; and fragmented prosecution may prevent a court from seeing how separate digital artefacts form a coherent narrative.

The model therefore treats forensic capacity as part of substantive criminal justice. It also requires institutional accountability: requests should be traceable, access should be auditable, preservation should be time-stamped, forensic tools should be validated and significant analytical limitations should be disclosed.

12. Comparative Perspective

Comparative analysis is useful when it identifies institutional principles rather than merely listing foreign statutes. European approaches provide important reference points for data protection and cross-border cooperation; the United Kingdom provides experience with digital-evidence practice and cybercrime enforcement; and United States practice offers significant examples concerning electronic communications, digital searches and cross-border evidence.

The comparative lesson is not that India should transplant foreign rules. India's constitutional structure, federal policing arrangements, population

scale and institutional design require domestic adaptation. The transferable principles are preservation, legality, necessity, proportionality, specialised expertise, provider cooperation, auditability and timely international evidence mechanisms.

For CLSR's international readership, the Indian case is significant because it illustrates a common regulatory problem: a state may modernise substantive criminal law without simultaneously harmonising evidence, forensic practice and institutional workflows. The post-2024 Indian framework is therefore a useful case study of legal interoperability in a large digital jurisdiction.

13. Critical Analysis

The central finding is that India's cybercrime framework is legally extensive but operationally fragmented. A single phishing incident may engage BNS liability, Information Technology Act provisions, BNSS procedure, BSA evidentiary rules, banking controls and data-governance requirements. Without common workflows, investigators may duplicate requests, collect inconsistent records or delay preservation.

The second finding concerns the nature of evidence. Statutory recognition of electronic records does not itself guarantee reliability. Reliability is produced through preservation, acquisition, integrity verification, provenance, attribution and transparent interpretation. This is why forensic quality should be treated as a justice-system capacity rather than a purely technical service.

The third finding concerns speed. In financial cybercrime, delay may permanently reduce the possibility of asset recovery. Rapid intervention should therefore be supported by clear authority, documentation and review mechanisms. The fourth concerns transnational evidence: cloud providers, exchanges and platforms may hold relevant records outside India, while logs may be volatile. Cross-border preservation and disclosure require greater procedural efficiency.

Finally, AI introduces a governance problem distinct from traditional digital evidence. Automated systems can improve efficiency while producing false positives, bias or opaque reasoning. Significant algorithmic outputs should therefore be accompanied by human verification, reproducible methodology and disclosure of material limitations.

14. Challenges

Shortage of trained cyber investigators and forensic specialists.

Uneven forensic infrastructure and quality-control practices.

Non-uniform procedures for preservation, seizure and forensic acquisition.

Encryption, anonymisation and identity-obfuscation technologies.

Cloud evidence and cross-border access difficulties.

Cryptocurrency tracing and rapid asset movement.

Deepfakes and synthetic evidence.

Difficulty establishing human attribution from technical traces.

Fragmentation between complaints, FIRs, forensic findings and prosecution.

Delays in obtaining information from platforms, banks and intermediaries.

Limited specialist capacity among prosecutors and judges.

Privacy, proportionality and data-security concerns.

Rapid technological evolution and corresponding legal uncertainty.

15. Recommendations

1. Adopt a national cybercrime investigation protocol integrating BNS, BNSS, BSA and Information Technology Act requirements.

2. Develop offence-specific investigative protocols for phishing, identity fraud, ransomware, online sexual offences, cryptocurrency fraud and synthetic media.

3. Provide foundational digital-evidence training for investigators and advanced specialist certification for forensic personnel.

4. Strengthen state and district forensic capacity through common quality standards, validation and accreditation.

5. Develop specialised cybercrime prosecution capacity and continuing judicial education.

6. Create interoperable, legally governed mechanisms among police, I4C, banks, telecommunications providers, platforms and forensic laboratories.

7. Improve rapid preservation and lawful disclosure mechanisms for evidence held outside India.

8. Establish an AI/deepfake evidence protocol requiring provenance assessment, tool validation, human review and disclosure of limitations.

9. Strengthen cryptocurrency investigations through blockchain analytics, exchange cooperation and lawful asset-preservation mechanisms.

10. Implement privacy-by-design safeguards, including role-based access, audit trails, purpose limitation and retention controls.

11. Publish separate statistical dashboards for complaints, FIRs, chargesheets, convictions, financial losses, recovery and technical incidents.

12. Support interdisciplinary research on forensic-tool reliability, evidentiary failure points and conviction outcomes.

16. Judicial Framework

[1] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 — foundational authority on electronic records under the former Section 65B framework.

[2] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 — clarified the certificate requirement under the former evidence regime.

[3] State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601 — recognised video-conferencing as a permissible means of taking evidence where procedural fairness is maintained.

[4] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178 — emphasised the importance of scientific and electronic evidence.

[5] Shreya Singhal v. Union of India, (2015) 5 SCC 1 — struck down Section 66A of the Information Technology Act and remains central to constitutional limits on online speech.

[6] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 — established privacy as a fundamental right and provides the constitutional foundation for proportionality in intrusive digital investigations.

[7] Sharat Babu Digumarti v. Government of NCT of Delhi, (2017) 2 SCC 18 — relevant to the interaction between the Information Technology Act and general criminal law concerning electronic publication.

[8] Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 603 — relevant to proportionality in regulation of cryptocurrency-related activity.

CONCLUSION

India's principal cybercrime challenge is not simply legislative insufficiency. The country has a substantial legal and institutional architecture comprising general criminal law, criminal procedure, electronic-evidence rules, technology-specific regulation, data governance and specialised institutions. The central challenge is integration.

The BNS supplies criminal liability for many forms of cyber-enabled conduct; the BNSS provides procedural architecture; the BSA regulates electronic and digital records; the Information Technology Act remains essential for specified technology-related conduct and intermediary regulation; and the DPDP framework introduces a data-governance dimension that must be reconciled with lawful investigative necessity. The effectiveness of these instruments depends on how they operate together.

The investigation-chain model proposed in this article offers a practical test: can an investigation move from complaint to classification, preservation, acquisition, forensic examination, attribution, financial or cross-border tracing, prosecution and adjudication without losing legality, integrity or explanatory coherence? If

not, additional offences alone are unlikely to solve the problem.

The broader lesson is internationally relevant. Contemporary cybercrime enforcement should be measured not only by the number of complaints registered or investigations opened, but by whether evidence is acquired lawfully, preserved reliably, interpreted transparently, attributed responsibly and presented in a manner capable of surviving adversarial scrutiny. A rights-sensitive, evidence-centred and institutionally interoperable model can strengthen both enforcement and the legitimacy of digital criminal justice.

GLOSSARY

BNS — Bharatiya Nyaya Sanhita, 2023.

BNSS — Bharatiya Nagarik Suraksha Sanhita, 2023.

BSA — Bharatiya Sakshya Adhiniyam, 2023.

DPDP Act — Digital Personal Data Protection Act, 2023.

I4C — Indian Cybercrime Coordination Centre.

CFCFRMS — Citizen Financial Cyber Fraud Reporting and Management System.

CERT-In — Indian Computer Emergency Response Team.

NCRB — National Crime Records Bureau.

REFERENCES

1. The Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023.
2. The Bharatiya Nagarik Suraksha Sanhita, 2023, Act No. 46 of 2023.
3. The Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023.
4. The Information Technology Act, 2000, Act No. 21 of 2000.
5. The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
6. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
7. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
8. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
9. State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
10. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
11. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
12. Sharat Babu Digumarti v. Government of NCT of Delhi, (2017) 2 SCC 18.
13. Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 603.
14. Constitution of India.
15. Digital Personal Data Protection Rules, 2025.
16. National Crime Records Bureau, Crime in India and relevant cybercrime reporting.
17. Indian Cybercrime Coordination Centre, Ministry of Home Affairs, National Cyber Crime Reporting Portal and CFCFRMS materials.
18. Indian Computer Emergency Response Team, relevant annual reporting.
19. Reserve Bank of India, Annual Report 2024–25.
20. Ratanlal & Dhirajlal, Law of Evidence.

HOW TO CITE: Lathika Karikalan K. M.*, Suresh Kumar R., Cybercrime Investigation in India after the 2023 Criminal-Law Reforms: Integrating Criminal Liability, Digital Evidence, Forensics and Institutional Enforcement, Int. J. Sci. R. Tech., 2026, 3 (8), 837-844. https://doi.org/10.5281/zenodo.22054549