INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE EPISTEMOLOGICAL CRISIS OF DIGITAL EVIDENCE: NAVIGATING INDIA'S TRANSITION TO THE BSA AND BNSS

AUTHOR – SHOBHITA SINGH* & DR. SHAIWALINI SINGH**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – SHOBHITA SINGH & DR. SHAIWALINI SINGH, THE EPISTEMOLOGICAL CRISIS OF DIGITAL EVIDENCE: NAVIGATING INDIA'S TRANSITION TO THE BSA AND BNSS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (4) OF 2026, PG. 184-195, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The enactment of India's new criminal justice framework comprising the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA) marks a paradigm shift in the legal validity and operational integration of digital evidence. However, this transition introduces a fundamental epistemological crisis, where the formalistic admissibility mandates of the BSA, such as the rigid dual certification requirement under Section 63, collide with severe infrastructural deficits, undertrained first responders, and a critical lack of accredited digital forensic experts.

Through a comparative analysis with mature adversarial jurisdictions like the United States and the United Kingdom, this research highlights India's lack of rigorous scientific gatekeeping (akin to the U.S. Daubert standard) and warns against the dangers of legally presuming computer reliability. Furthermore, the study explores a "Privacy Paradox" exacerbated by the broad state exemptions under Section 17 of the Digital Personal Data Protection (DPDP) Act. Unlike Western constitutional protections, this framework lacks a statutory "right to deletion" for non-responsive seized data, threatening to establish an unchecked surveillance architecture.

To bridge the gap between statutory intent and forensic reality, this paper advocates for the adoption of international protocols (ISO/IEC 27037 and NIST SP 800-86) alongside "trustless" technological architectures. Specifically, it proposes a Hybrid Blockchain-IPFS model to maintain a scalable, privacy-preserving, and immutable chain of custody for digital evidence. Ultimately, the research recommends strategic reforms including judicial gatekeeping for forensic tools, national expert accreditation, and a statutory mandate for data deletion to ensure that India's digital-first justice system remains rigorous, transparent, and respectful of constitutional privacy rights.

Key words: Digital Evidence, Bharatiya Sakshya Adhiniyam (BSA), Scientific Gatekeeping Privacy Paradox, Chain of Custody

1.1 Introduction: The Epistemological Crisis of Digital Evidence

The preceding Research paper delineated the doctrinal evolution of India's evidentiary regime, tracing the transition from the colonial-era Indian Evidence Act, 1872 (IEA), to the modern triad of the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA), 2023. While Research paper established the *legal* validity of

electronic records, elevating them from secondary afterthoughts to primary documentary evidence, Research paper 5 also interrogates the *operational* feasibility of this paradigm shift. This Research paper serves as the critical bridge between statutory intent and forensic reality, examining whether the Indian criminal justice system possesses the institutional, technical, and procedural capacity to uphold the mandates of the new Sanhitas.

The integration of digital evidence into the courtroom is not merely a matter of updating statutes; it represents a fundamental epistemological rupture. Traditional evidence, such as a bloodstained knife, a handwritten letter, and a witness testimony, possesses a physical persistence and a direct chain of causality that the human senses can interrogate. Digital evidence, by contrast, is latent, mutable, and mediated. It consists of magnetic fluxes and voltage states that must be interpreted by complex, often proprietary, algorithms before they can be rendered intelligible to a judge. This mediation introduces a "crisis of credibility," in which the evidence's provenance is perpetually suspect unless bolstered by rigorous forensic hygiene.[330]

As India accelerates its digital transformation, with over a billion active mobile connections and a burgeoning digital economy, the volume of digital traces, from UPI transaction logs to GPS metadata, has increased substantially. The BNSS responds to this by mandating audio-visual recording of search and seizures (Section 105) and expanding the scope of forensic examination.[331] However, this legislative ambition collides with a stark infrastructural reality: a chronic shortage of forensic laboratories, a lack of standardised procedural protocols, and a judiciary often ill-equipped to scrutinise the "black box" of digital forensics. Furthermore, the sweeping exemptions granted to law enforcement under the Digital Personal Data Protection Act, 2023 (DPDP Act), create tension between state efficiency and citizen privacy, which threatens to undermine the legitimacy of the very evidence the state seeks to admit.[332]

This Research paper is structured to provide an exhaustive analysis of these tensions. It begins by dissecting the implementation challenges of the BSA and BNSS, focusing on the "validity vs. admissibility" dichotomy. It then proceeds to a granular comparative analysis, juxtaposing India's emerging framework against the mature digital jurisprudence of the United States (specifically the *Daubert* standard and Fourth Amendment protections), the United Kingdom (the *PACE* framework and the lessons of the Horizon Post Office scandal), and the European Union. Finally, it examines the technological architectures necessary to bridge the trust gap, evaluating the efficacy of blockchain-based chains of custody (as piloted by the Delhi Police) and the adoption of international standards such as ISO/IEC 27037 and NIST SP 800-86.

1.2 The Statutory Mandate and the Implementation Gap

The enactment of the Bharatiya Sakshya Adhiniyam (BSA) and the Bharatiya Nagarik Suraksha Sanhita (BNSS) in 2023 marked a watershed moment in Indian legal history. These laws were designed to decolonise the criminal justice system and integrate technology into the core of investigative procedures. However, the transition from the "law in books" to the "law in action" reveals profound structural fissures.

1.2.1 Section 63 BSA: The Certification Conundrum

Section 63 of the BSA replaces the contentious Section 65B of the IEA, which had been the subject of vacillating judicial interpretation for two decades, culminating in the Supreme Court's ruling in *Arjun Panditrao Khotkar v.*

[330] *See* Stephen Mason, "The presumption that computers are 'reliable'", in *Electronic Evidence and Electronic Signatures* (5th edn, University of London 2021); *See also* "Comparative Analysis of Admissibility and Relevance of Electronic and Digital Evidence", 4 *International Journal of Integrated Research in Law* 1 (2022).

[331] The Bharatiya Nagarik Suraksha Sanhita, 2023, s. 105.

[332] The Digital Personal Data Protection Act, 2023, s. 17.

Kailash Kushanrao Gorantyal.[333] The new provision is intended to simplify the admissibility of electronic records but introduces procedural complexities that could create bottlenecks in the trial process.[334]

The Dual Certification Requirement:

Unlike its predecessor, Section 63 explicitly mandates a more rigorous certification regime. It requires not only a certificate from the person responsible for the computer system (Section 63(2)) but also the appointment of an "expert" in the validation process (Section 63(4)).[335] The certificate must now include granular technical details:

- The **hash value** of the electronic record, specifying the algorithm used (e.g., MD5, SHA-256).
- The **device specifications**, including make, model, serial number, and unique identifiers like IMEI or MAC addresses.
- A declaration of the **integrity of the system**, affirming that the device was operating properly during the material period.[336]

While these requirements appear robust on paper, they presuppose a level of technical literacy that is currently absent in the lower rungs of the police force and the judiciary. The requirement for an "expert" certificate is particularly problematic. The BSA expands the definition of an expert to include "any other field," yet it fails to establish a statutory accreditation body for digital forensic experts. This leaves the door open to "junk science," in which individuals with dubious qualifications may certify complex digital evidence, or, conversely, in which valid evidence is excluded because a legitimate expert lacks a formal government designation.[337]

The Burden on Parties:

The BSA distinguishes between certificates provided by the party (Part A) and those offered by the expert (Part B). This bifurcation places a significant burden on private litigants who may not have access to forensic experts to certify their own digital communications (e.g., WhatsApp chats in a divorce proceeding). The "certificate by the party" requires them to provide technical details like hash values, which an average citizen is incapable of generating without specialised software. This could effectively bar valid exculpatory evidence from admission due to technical non-compliance, thereby violating the principles of a fair trial.[338]

1.2.2 The Infrastructural Deficit: A Case Study of Systemic Strain

The BNSS mandates the extensive use of forensic science in investigations, particularly for offences punishable by seven years or more (Section 173). It also creates a statutory obligation to audio-visual record crime scenes and search proceedings (Section 105) to ensure transparency.[339]

The Capacity Crisis:

Implementation of these mandates requires a massive scaling of forensic infrastructure. Current data indicate a severe deficit. For instance, in the state of Bihar, a jurisdiction with over 100 million people, the forensic infrastructure is critically insufficient. The State Forensic Science Laboratory (SFSL) in Patna is overburdened, with support from only two regional laboratories in Bhagalpur and Muzaffarpur.[340] This scarcity leads to massive backlogs. When a digital device is seized, it may

[333] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[334] "Electronic Records Now Governed by Section 63 of the Bhartiya Sakshya Adhiniyam, 2023", *R.K. Dewan & Co.*, *available at*: https://www.rkdewan.com/articles/electronic-records-now-governed-by-section-63-of-the-bhartiya-sakshya-adhiniyam-2023/ (last visited on Jan. 2026).
[335] The Bharatiya Sakshya Adhiniyam, 2023, s. 63(4).
[336] *Ibid*, s. 63(2).
[337] *See* "Guest Post: Expert Certificates, BSA, and the 'Expert' Conundrum", *The Proof of Guilt*, *available at*: https://theproofofguilt.blogspot.com/2025/08/guest-post-expert-certificates-bsa-and.html (last visited on Jan. 2026).
[338] The Bharatiya Sakshya Adhiniyam, 2023, s. 63(4)(c) (Schedule Part A).
[339] The Bharatiya Nagarik Suraksha Sanhita, 2023, s. 105; *See also* s. 173.
[340] "Bharatiya Nagarik Suraksha Sanhita digital evidence implementation challenges", *International Journal for Multidisciplinary Research*, *available at*: https://www.ijfmr.com/papers/2025/5/55301.pdf (last visited on Jan. 2026).

remain in a queue for months or years before being imaged, during which time volatile data may degrade, or the chain of custody may be compromised.

The "Data Gravity" of Section 105:

The requirement to videograph search and seizure operations creates a "data gravity" problem. A single high-definition video of a raid can occupy several gigabytes. If every police station in India complies with this mandate daily, the system will generate petabytes of data annually. The BNSS is silent on the storage architecture for this data.

- Where will this data be stored? (Local hard drives, state data centres, or commercial clouds?)
- How will it be secured against tampering?
- How will it be retrieved years later during the trial?

Without a dedicated, secure cloud infrastructure, Section 105 risks becoming a performative exercise in which videos are recorded but are lost, corrupted, or inadmissible due to broken chains of custody.[341]

1.2.3 The Human Capital Crisis and Judicial Competence

The most significant barrier to implementation is not hardware, but "humanware." The effective handling of digital evidence requires specialised training that treats digital data with the same degree of fragility as biological samples.

First Responder Incompetence:

Police officers, who act as first responders, often lack the training to handle digital crime scenes. Common errors include:

- Turning on a seized device, which alters timestamps and system logs.
- Failing to isolate the device from the network (Faraday bags), allowing remote wiping by the suspect.
- Using non-forensic methods to copy data (e.g., drag-and-drop), which destroys metadata and alters hash values.

The legal community has expressed grave concerns that the "nationwide lack of resources and training" will lead to the mismanagement of evidence, resulting in acquittals not based on innocence but due to procedural incompetence.[342]

Judicial Blind Spots:

The judiciary faces a similar competence gap. Judges are now required to adjudicate on the admissibility of complex digital artefacts, including encrypted messaging logs, geolocation data, and blockchain transaction histories. Without mandatory, continuous training on the nuances of digital forensics (e.g., understanding the difference between "deleted" and "overwritten" data, or the probabilistic nature of AI-based evidence), courts risk making rulings based on technically flawed analogies. The Vidhi Centre for Legal Policy notes that, rather than ensuring reliability, the dual certification process may lead to "superficial compliance," in which judges check for the presence of a certificate rather than interrogating the veracity of the evidence it purports to authenticate.[343]

1.3 Comparative Analysis: India in the Global Forensic Context

To accurately assess the trajectory of India's digital evidence framework, it is instructive to benchmark it against mature adversarial jurisdictions. This comparison reveals divergent philosophies regarding admissibility, scientific

[341] *Ibid.*

[342] *See* "Revolutionizing Criminal Investigations: The Forensic Mandate under Section 176 of BNSS", *International Journal of Law and Legal Research* (2025).

[343] Mayank Khichar, "The Evolving Enigma: A Case for 'Digital Evidence' under the Bharatiya Sakshya Adhiniyam, 2023", *Vidhi Centre for Legal Policy*, *available at*: https://vidhilegalpolicy.in/blog/the-evolving-enigma/ (last visited on Jan. 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

reliability, and the balance between state power and individual privacy.

1.3.1 Admissibility Regimes: Formalism vs. Reliability

United States: The Rule of Reliability:

The United States Federal Rules of Evidence (FRE) prioritise substantive reliability over procedural formalism. Rule 901(b)(9) allows for the authentication of digital evidence through "evidence describing a process or system and showing that it produces an accurate result." This flexible standard accommodates evolving technologies without requiring legislative amendments.

- *Case Law - United States v. Lizarraga-Tirado:* In this landmark case, the Ninth Circuit addressed whether a Google Earth satellite image with a digital "tack" (marker) constituted hearsay. The defence argued that the tack was an out-of-court statement. The court ruled that the tack was not hearsay because it was machine-generated. "The program analyses the GPS coordinates and, without any human intervention, places a labelled tack… The computer program itself does the real work".[344] This ruling established that machine assertions are matters of *process reliability*, not witness credibility. The court focused on whether the *system* worked, not whether a specific certificate was filed.[345]

United Kingdom: Discretion and Fairness:

The UK operates under the Police and Criminal Evidence Act 1984 (PACE). Section 78 gives courts the discretion to exclude evidence if its admission would "unfairly affect the fairness of the proceedings." This allows judges to exclude digital evidence if its provenance is in doubt, even if it is technically relevant. This discretionary power serves as a safeguard against police misconduct or forensic incompetence.[346]

India: The Certificate as Gatekeeper:

In contrast, India's approach under Section 63 BSA is heavily formalistic. The admissibility of electronic evidence is contingent upon the production of a certificate. While the Supreme Court in Arjun Panditrao clarified that the certificate is a condition precedent, the rigid adherence to this form often leads to a "form over substance" approach. A perfectly reliable piece of evidence may be excluded for want of a certificate, while a fabricated record may be admitted if accompanied by a correctly filled (but fraudulent) certificate. The BSA's emphasis on the document (the certificate) rather than the process (the forensic methodology) diverges from the global trend toward examining the scientific validity of the evidence.[347]

1.3.2 The Gatekeeping of Scientific Expertise: Daubert vs. Section 45

The standard for admitting expert testimony is a critical differentiator in forensic quality control.

The Daubert Standard (USA):

Since 1993, US federal courts have applied the Daubert v. Merrell Dow Pharmaceuticals standard, which designates the judge as a "gatekeeper" of scientific validity. For forensic evidence to be admissible, the methodology must satisfy four criteria:

1. **Testability:** Can the technique be tested?
2. **Peer Review:** Has it been subjected to peer review and publication?
3. **Error Rate:** Is the known or potential error rate acceptable?

[344] *United States v. Lizarraga-Tirado*, 789 F.3d 1107 (9th Cir. 2015).
[345] *Ibid.*
[346] Police and Criminal Evidence Act 1984, s. 78 (UK).
[347] *See* "Digital Evidence & Due Process: A Comparative Analysis", *Record of Law*, *available at*: https://recordoflaw.in/digital-evidence-due-process-a-comparative-analysis-of-fairness-in-criminal-trials-in-the-united-states-and-united-kingdom/ (last visited on Jan. 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

4. General Acceptance: Is the technique accepted in the relevant scientific community?[348]

These standards force prosecutors to demonstrate that the digital forensic tools (e.g., EnCase, Cellebrite) used are scientifically sound. It prevents "black box" forensics, where an expert says "the machine said so" without explaining how the machine works.

The Indian Context (Section 45/BSA):

India lacks a statutory equivalent to the Daubert standard. Section 45 of the IEA (and the corresponding BSA provision) allows for expert opinion but does not mandate an inquiry into the methodology used. Consequently, Indian courts rarely question the algorithms or error rates of forensic software. Reports from government laboratories are often treated as infallible. This "institutional trust" model is dangerous in the digital age, where software bugs can produce erroneous results that look authentic. The lack of a Daubert-like filter allows "junk science" to enter the courtroom, provided it comes from a recognised government lab.[349]

1.3.3 The Dangers of Presumption: The Horizon Post Office Scandal

A cautionary tale for India lies in the UK's experience with the legal presumption of computer reliability.

The Presumption:

Following the Law Commission's 1997 recommendations, English courts adopted the presumption that "in the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time".[350] This effectively reversed the burden of proof, requiring defendants to prove that the computer was broken.

The Scandal:

In Bates v. Post Office Ltd, this presumption facilitated a massive miscarriage of justice. The Post Office's "Horizon" accounting software contained bugs that generated false financial shortfalls. Because of the legal presumption, the Post Office was not required to prove the system's integrity. Sub-post managers, who lacked access to the source code or backend logs, could not rebut the presumption and were wrongfully convicted of theft.[351]

Implications for the BSA:

India's Section 63(2) BSA contains an implicit presumption of reliability, requiring a statement that the device was "operating properly." If Indian courts adopt a rigid interpretation akin to the pre-Bates UK position, it could disastrously shift the burden to the accused, in a country where the digital divide is stark, expecting an accused person to prove that a police computer or a banking algorithm malfunctioned is practically impossible. The Bates judgment serves as a stark warning: legal presumptions of technological infallibility are incompatible with the complex, bug-prone nature of modern software.[352]

1.3.4 Constitutional Protections: The Fourth Amendment vs. DPDP Act Exemptions

The tension between forensic acquisition and privacy rights represents the deepest divergence between India and the West.

US: The Fourth Amendment and the "Mirroring" Problem:

In the US, the Fourth Amendment protects against "unreasonable searches and seizures." This has led to robust jurisprudence regarding digital devices.

- *United States v. Ganias*: The Second Circuit held that the government violated the Fourth Amendment by retaining forensic mirror images of hard drives for over two years and searching

[348] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

[349] Pranav Saraf, "The Politics of Proof", *Vidhi Centre for Legal Policy*, *available at*: https://vidhilegalpolicy.in/blog/the-politics-of-proof/ (last visited on Jan. 2026)

[350] Law Commission of England and Wales, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997).

[351] *Bates v. Post Office Ltd (No 6: Horizon Issues)*, EWHC 3408 (QB).

[352] Stephen Mason, "The presumption that computers are reliable", *Counsel Magazine*, *available at*: https://www.counselmagazine.co.uk/articles/the-presumption-that-computers-are-reliable (last visited on Jan. 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

them for crimes unrelated to the original warrant. This established a "right to deletion" for non-responsive data found in forensic images.[353]

- *Riley v. California*: The Supreme Court ruled that police must obtain a warrant to search a cell phone seized incident to arrest, recognising that modern phones contain the "privacies of life".[354]

India: The DPDP Act and the Surveillance State:

India's legal framework moves in the opposite direction. The Digital Personal Data Protection Act, 2023 (DPDP Act), while establishing a privacy regime, carves out sweeping exemptions for the state.

- **Section 17 Exemptions:** Section 17(1)(c) exempts the processing of personal data from the Act's core obligations (notice, consent, purpose limitation) when it is for the "prevention, detection, investigation, or prosecution of any offence".[355]
- **Implications:** unlike the US *Ganias* standard, there is no statutory requirement in India for police to delete non-responsive data from seized devices. The broad wording of Section 17 allows law enforcement to retain forensic images indefinitely and potentially mine them for intelligence, creating a "panopticon" effect. Critics argue this establishes an "alternate regime" for the state, untethered from the oversight mechanisms that bind private data fiduciaries.[356] This lack of procedural safeguards violates the proportionality principles established in the *Puttaswamy* judgment.

Table 1.1: Comparative Analysis of Digital Evidence Frameworks

Dimension	India (BSA/BNSS/DPDP)	United States (FRE/4th Amendment)	United Kingdom (PACE/Common Law)
Admissibility Standard	**Formalistic:** Mandatory dual certification (Sec 63 BSA).	**Reliability-Based:** Authentication of process (Rule 901); machine output is not hearsay (*Lizarraga-Tirado*).	**Discretionary:** Fairness test (Sec 78 PACE); judicial discretion to exclude.
Scientific Gatekeeping	**Weak:** Sec 45 allows expert opinion but no statutory test for methodology.	**Strong:** *Daubert* standard requires validation, error rates, and peer review of tools.	**Moderate:** Law Commission presumption of reliability (now challenged post-*Bates*).
Search & Seizure	**Broad:** Sec 94 BNSS allows wide seizure; Sec 17 DPDP exempts the state	**Restricted:** Warrant required for phones (*Riley*); retention of non-	**Regulated:** PACE codes of practice; judicial oversight of surveillance.

[353] *United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014).
[354] *Riley v. California*, 573 U.S. 373 (2014).
[355] The Digital Personal Data Protection Act, 2023, s. 17(1)(c)
[356] "Between Consent and Control: A Critical Analysis of India's DPDP Act, 2023", *Record of Law*, *available at*: https://recordoflaw.in/between-consent-and-control-has-india-fulfilled-its-constitutional-promise-a-critical-analysis-of-indias-dpdp-act-2023/ (last visited on Jan. 2026).

	from purpose limitation.	responsive data prohibited (*Ganias*).	
Privacy Safeguards	**Exemptions:** State agencies are largely exempt from data protection obligations (Sec 17 DPDP).	**Constitutional:** 4th Amendment protects "reasonable expectation of privacy" (*Carpenter*).	**Statutory:** GDPR/Data Protection Act 2018 (law enforcement processing must be necessary/proportionate).

1.4 Technological Architectures for Forensic Integrity

Given the structural weaknesses and legal risks identified above, relying solely on traditional procedural safeguards is insufficient. India must leverage technology to enforce the integrity that the bureaucracy struggles to maintain. This section explores the "Trustless" architectures, specifically Blockchain and standards-based workflows, that can operationalise the BSA's mandates.

1.4.1 Standardisation: The ISO/IEC 27037 and NIST SP 800-86 Frameworks

To align with global standards and ensure the cross-border admissibility of evidence (crucial in cybercrime cases), India must adopt international protocols for the digital handling of evidence.

ISO/IEC 27037:

This standard provides guidelines for the "identification, collection, acquisition, and preservation of digital evidence." It is designed to facilitate the exchange of evidence between jurisdictions.

- **Key Mandate:** It requires that the handling of digital evidence be auditable and repeatable. If a different expert follows the same process, they should achieve the same result.
- **Application:** Adopting ISO/IEC 27037 in Indian State Forensic Labs (SFSLs) would standardise the "acquisition" phase, ensuring that the hash values recorded in the BSA certificate are generated using globally validated methods.[357]

NIST SP 800-86:

The National Institute of Standards and Technology (NIST) guide offers a comprehensive workflow for integrating forensics into incident response. It delineates four phases:

1. **Collection:** Identifying and acquiring data while preserving integrity. NIST emphasises the "order of volatility" (capturing RAM before hard drives).[358]
2. **Examination:** Using automated tools to extract data.
3. **Analysis:** Interpreting the data to answer investigative questions.
4. Reporting: Presenting findings.

Notably, NIST SP 800-86 recommends proactive measures, including maintaining a National Software Reference Library (NSRL) of known file hashes. This allows investigators to quickly filter out "known good" files (such as Windows system files) and focus solely on user-generated data, thereby significantly reducing the analysis backlog.[359]

1.4.2 Blockchain-Based Chain of Custody: The Delhi Police Model

The "Chain of Custody" (CoC) is the weakest link in Indian forensics. Paper logs can be lost, rewritten, or forged. Blockchain technology

[357] ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.*
[358] NIST Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response* (National Institute of Standards and Technology, 2006).
[359] *Ibid.*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

offers a solution by creating an immutable, distributed ledger for evidence handling.

The Delhi FSL Pilot:

The Delhi Forensic Science Laboratory has implemented a blockchain system utilising Distributed Ledger Technology (DLT) to track evidence.

- **Mechanism:** When evidence is collected, it is assigned a QR code. The initial state (including the hash of the evidence metadata) is recorded as a block on the ledger.
- **Tracking:** Every subsequent movement transfer to the *Malkhana* (evidence locker), handover to the constable, receipt at the lab, and opening for analysis is recorded as a transaction.
- **Immutability:** The blockchain ensures that no entry can be retroactively altered. If a police officer attempts to modify the timestamp of a seizure, the block hash would change, breaking the chain and alerting the network.[360]
- **Architecture:** The system uses a permissioned blockchain where the Police, FSL, and the Judiciary control nodes. This prevents unauthorised public access while ensuring transparency among the stakeholders.[361]

Critique and Scalability:

While the Delhi model addresses the integrity of metadata, it faces scalability challenges with respect to the underlying data. Storing terabytes of forensic images on a blockchain is technically infeasible due to block size limits and network latency.

1.4.3 The Hybrid Architecture: Blockchain + IPFS

To address scalability issues, a hybrid architecture is proposed that combines Blockchain with the InterPlanetary File System (IPFS).

Technical Workflow:

1. **Off-Chain Storage (IPFS):** The heavy digital evidence (e.g., a 500GB hard drive clone) is encrypted and stored on IPFS, a decentralised, content-addressable storage network. IPFS generates a Content Identifier (CID), which is a cryptographic hash of the file itself.[362]
2. **On-Chain Anchor (Blockchain):** Only the CID, along with the access control metadata (who uploaded it, permissions), is stored on the blockchain smart contract.
3. **Verification:** To verify integrity in court, the expert retrieves the file from IPFS. The system automatically recalculates the hash. If it matches the CID stored on the immutable blockchain, the evidence is authenticated.
4. **Privacy-Preserving Access:** Sensitive data (e.g., medical records) is encrypted using AES-256-GCM. Access keys are managed by smart contracts, ensuring that only authorised personnel (e.g., the investigating officer or the judge) can decrypt the file. This architecture technically enforces the privacy protections that the DPDP Act fails to provide.[363]

Table 1.2: Technological Solutions to Forensic Challenges

Challenge	Technological Solution	Mechanism	Benefit
Tampered Chain of	**Blockchain Ledger (Delhi**	Immutable recording of	Prevents retroactive

[360] "Blockchain to track forensic custody in Delhi", *Ledger Insights* (Aug. 21, 2023), *available at*: https://www.ledgerinsights.com/blockchain-track-forensic-custody-delhi/ (last visited on Jan. 2026).
[361] *Ibid.*
[362] "Hybrid Blockchain Architecture for Digital Evidence", 8 *International Journal of Recent Technology and Engineering* 1 (2019).
[363] "A Scalable and Privacy Preserving Hybrid Blockchain Architecture", 16 *The SAI Organization* 8 (2025), *available at*: https://thesai.org/Downloads/Volume16No8/Paper_95-A_Scalable_and_Privacy_Preserving_Hybrid_Blockchain_Architecture.pdf (last visited on Jan. 2026).

Custody	**Model)**	evidence movement steps.	alteration of logs; establishes trust.
Storage Scalability	**Hybrid IPFS + Blockchain**	Store large datasets on IPFS; store the hash/CID on the Blockchain.	efficient storage of petabytes of data without bloating the ledger.
Data Validity	**NIST/ISO Standards**	Standardised hashing and acquisition protocols.	Ensures evidence is admissible in cross-border jurisdictions.
Privacy Violation	**Smart Contract Access Control**	Cryptographic key management for data access.	technically enforces "need to know" access, mitigating "surveillance state" risks.

1.5 The Privacy Paradox: Section 17 and the Erosion of Rights

The implementation of digital forensics in India cannot be viewed in isolation from the broader privacy landscape. The interaction between the BNSS's investigative powers and the DPDP Act's exemptions creates a "Privacy Paradox."

The Exemption Regime:

Section 17 of the DPDP Act provides a "blanket exemption" for state instrumentalities in the interest of sovereignty, security, and public order. Unlike the GDPR (Article 23), which requires such exemptions to be "necessary and proportionate" and subject to specific safeguards, Section 17 removes the oversight of the Data Protection Board for law enforcement activities.[364]

Impact on Forensics:

This exemption regime fundamentally alters the forensic landscape.

1. **Lack of Purpose Limitation:** Police can collect data for a traffic violation investigation and retain it indefinitely for other purposes. This accumulation of data creates "honey pots" of citizen information that are vulnerable to breach and misuse.[365]
2. **Erosion of Trust:** If citizens believe that any interaction with the police will result in the permanent seizure and surveillance of their digital lives, they will be less likely to cooperate with investigations or report cybercrimes.
3. **Legal Risk:** While the DPDP Act allows this, constitutional challenges based on *Puttaswamy* (Right to Privacy) are inevitable. Evidence obtained through mass, indiscriminate surveillance authorised under Section 17 may ultimately be struck down by the Supreme Court as disproportionate, rendering the forensic effort futile.

1.6 Conclusion and Strategic Roadmap

The analysis of Research paper 5 reveals that the operationalisation of digital forensics in India is a project of immense complexity, fraught with structural, legal, and ethical perils. The BSA and BNSS provide the necessary statutory scaffolding, but the edifice is shaky.

[364] General Data Protection Regulation (EU) 2016/679, art. 23.
[365] "India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison", *Latham & Watkins*, *available at*: https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf (last visited on Jan. 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Key Findings:

- **The Credibility Gap:** The lack of *Daubert*-style gatekeeping and the reliance on formalistic certificates (Section 63 BSA) risks creating a justice system that trusts machines more than it interrogates them.
- **The Infrastructural Chasm:** The forensic capacity in states like Bihar is nowhere near the level required to support the BNSS's mandates, threatening to collapse the trial process under the weight of backlogs.
- **The Privacy Vacuum:** The expansive exemptions under Section 17 DPDP Act, combined with the lack of a "right to deletion" for seized data (unlike *US v. Ganias*), establish a surveillance architecture that may be constitutionally vulnerable.
- **The Technological Imperative:** Traditional methods are obsolete. The adoption of Blockchain-based chains of custody (as pioneered in Delhi) and Hybrid IPFS architectures is not optional but existential for the integrity of digital evidence.

Strategic Recommendations:

1. **Judicial Gatekeeping Reform:** The Supreme Court should read a *Daubert*-like reliability test into Section 45/63 of the BSA, empowering judges to question the error rates and validation of forensic tools.
2. **Statutory "Right to Deletion":** The BNSS should be amended to explicitly mandate the deletion of non-responsive data from forensic images after the conclusion of a trial, closing the loophole left by the DPDP Act.
3. **National Blockchain Standard:** The Ministry of Home Affairs should standardise the Delhi Police blockchain pilot into a National Digital Evidence Backbone, interoperable across all states and courts.
4. **Accreditation of Experts:** A central body must be established to accredit digital forensic experts, ensuring that the "experts" certifying evidence under Section 63 BSA are technically competent and ethically bound.

In the final analysis, the transition to a digital-first criminal justice system is not merely a technical upgrade; it is a renegotiation of the social contract. If India can build a forensic infrastructure that is rigorous, transparent, and privacy-respecting, it can set a global benchmark. If it fails, it risks automating injustice.

BIBLIOGRAPHY

Indian Statutes and Legislation

- **Bharatiya Nyaya Sanhita (BNS), 2023**.
- **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023** (Specifically Sections 94, 105, and 173).
- **Bharatiya Sakshya Adhiniyam (BSA), 2023** (Specifically Sections 45 and 63).
- **Digital Personal Data Protection Act (DPDP), 2023** (Specifically Section 17).
- **Indian Evidence Act, 1872 (IEA)** (Specifically Sections 45 and 65B).

International Statutes and Legislation

- **United States Constitution**, Fourth Amendment.
- **United States Federal Rules of Evidence (FRE)** (Specifically Rule 901(b)(9)).
- **Police and Criminal Evidence Act 1984 (PACE)**, United Kingdom (Specifically Section 78).
- **General Data Protection Regulation (GDPR)**, European Union (Specifically Article 23).
- **Data Protection Act 2018**, United Kingdom.

Indian Case Laws

- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, Supreme Court of India (addressing the mandatory nature of certification for electronic records).
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, Supreme Court of India (establishing the constitutional right to privacy and proportionality principles).

International Case Laws

- *Daubert v. Merrell Dow Pharmaceuticals*, United States Supreme Court, 1993 (establishing the standard for admitting expert scientific testimony).
- *United States v. Lizarraga-Tirado*, Ninth Circuit, United States (ruling on machine-generated evidence and process reliability).
- *United States v. Ganias*, Second Circuit, United States (establishing limits on retaining non-responsive data from forensic images under the Fourth Amendment).
- *Riley v. California*, United States Supreme Court (requiring a warrant to search a seized cell phone).
- *Carpenter v. United States*, United States Supreme Court (protecting the reasonable expectation of privacy under the Fourth Amendment).
- *Bates v. Post Office Ltd*, United Kingdom (highlighting the dangers of legally presuming computer and software reliability).

International Standards and Guidelines

- **ISO/IEC 27037**: International standard providing guidelines for the identification, collection, acquisition, and preservation of digital evidence.
- **NIST SP 800-86**: National Institute of Standards and Technology guide to integrating forensic techniques into incident response.

Reports, Institutions, and Technical Frameworks

- **Law Commission (United Kingdom)**: 1997 recommendations regarding the presumption of computer reliability.
- **Vidhi Centre for Legal Policy**: Cited for expressing concerns that dual certification may lead to "superficial compliance" by judges.
- **National Software Reference Library (NSRL)**: Recommended by NIST for maintaining a database of known file hashes to filter "known good" files during investigations.