THE AUTHENTICATION PARADOX: INDIA'S TRIPARTITE EVIDENTIARY DEFICIT IN DATA BREACH LITIGATION AND THE CASE FOR A FORENSIC AUTHENTICITY FRAMEWORK

Samarth Udasin, National Law Institute University, Bhopal

Rishabh Sisodiya, National Law Institute University, Bhopal

Priyanshu Tripathi, National Law Institute University, Bhopal

ABSTRACT

The intersection of forensic science and evidentiary law in data breach litigation presents what this paper terms the *Authentication Paradox*: India's tripartite legislative framework — comprising the Bharatiya Sakshya Adhiniyam 2023 (BSA), the Digital Personal Data Protection Act 2023 (DPDPA), and the Information Technology Act 2000 (IT Act) — simultaneously mandates the use of digital artifacts as evidence of breach while failing to establish a coherent, judicially administrable methodology for authenticating those same artifacts. The BSA 2023 modernises the evidentiary regime for electronic records through its successor to Section 65B certification, yet operates in structural isolation from the DPDPA 2023's mandatory breach notification architecture, which generates a distinct class of documentary evidence whose evidentiary status courts have not been called upon to evaluate. Simultaneously, the IT Act's penalization provisions demand a forensic standard of proof that neither statute adequately supplies. Drawing on a comparative analysis of the Council of Europe's Convention on Cybercrime (Budapest Convention), NIST Special Publication 800-86, ISO/IEC 27037:2012, and the ACPO Good Practice Guide for Digital Evidence, this paper diagnoses three structural deficits and proposes the *Forensic Authenticity Framework* (FAF) — a three-tier doctrinal standard comprising Technical Integrity Assessment, Procedural Compliance Verification, and Contextual Reliability Evaluation — as the basis for an internationally harmonized approach to forensic evidence in Indian data breach litigation. The paper further argues that the FAF is constitutionally necessary to give meaningful content to the right to an effective remedy for informational privacy violations recognized under Article 21 in *KS Puttaswamy v Union of India* (2017) 10 SCC 1.

Keywords: Authentication Paradox; Forensic Authenticity Framework; Bharatiya Sakshya Adhiniyam 2023; DPDPA 2023; Section 65B; Digital

Forensics; Data Breach Litigation; Chain of Custody; Cybercrime Prosecution; Tripartite Evidentiary Deficit.

I. INTRODUCTION

The prosecution of cybercrime in India has, for the better part of two decades, been constrained by a tension that courts have navigated by instinct rather than by principle: digital evidence is simultaneously indispensable to proving data breach offences and structurally resistant to the authentication norms that the Indian law of evidence has historically demanded. The codification of the Bharatiya Sakshya Adhiniyam 2023[1] represented an opportunity to resolve this tension comprehensively. That opportunity has been only partially seized. By focusing almost exclusively on the admissibility of electronic records as reproductions of documentary evidence, and by retaining (in substantially modified form) the certification mechanism inherited from Section 65B of the Indian Evidence Act 1872, the BSA 2023 perpetuates what this paper characterises as an *Authentication Paradox*.

The paradox operates at a structural level. On one hand, the volume of data breach incidents in India creates an acute and growing demand for forensic evidence in both civil and criminal proceedings. CERT-In reported 1,39,294 cybersecurity incidents in 2023[2] — a trajectory that places forensic authentication at the heart of an ever-expanding docket of cybercrime litigation. On the other hand, the legal infrastructure for evaluating, receiving, and weighing such evidence remains fragmented across three legislative instruments that were not designed to operate as a coherent evidentiary ecosystem: the Information Technology Act 2000[3] (which creates the primary criminal offences); the Digital Personal Data Protection Act 2023[4] (which imposes substantive data protection obligations and breach notification requirements); and the BSA 2023 (which governs evidence admissibility). The product of this fragmentation is a tripartite evidentiary deficit that manifests at three analytically distinct levels: forensic methodology, statutory interoperability, and judicial capacity.

This paper proceeds in seven further parts. Part II maps the tripartite legislative architecture and identifies the functional purpose of each instrument in the data breach

[1]Bharatiya Sakshya Adhiniyam 2023 (No 46 of 2023) (BSA 2023), which came into force on 1 July 2024 repealing the Indian Evidence Act 1872.
[2]CERT-In, Annual Report 2023 (Ministry of Electronics and Information Technology 2024) 14. India recorded 1,39,294 cybersecurity incidents in 2023, representing a significant increase from prior years.
[3]Information Technology Act 2000 (No 21 of 2000) (IT Act).
[4]Digital Personal Data Protection Act 2023 (No 22 of 2023) (DPDPA 2023).

litigation ecosystem. Part III examines the forensic-evidentiary interface, focusing on the mechanisms by which forensic evidence is generated, preserved, and presented in breach cases, and identifies the Certification Bottleneck as the central procedural pathology of the current framework. Part IV charts the judicial trajectory of India's digital evidence jurisprudence, from *State (NCT of Delhi) v Navjyot Sandhu* (2005) through *Anvar PV v PK Basheer* (2014) to the watershed judgment in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020). Part V diagnoses the Authentication Paradox in detail, articulating the three structural deficits that undermine effective forensic evidence use in breach litigation. Part VI surveys comparative frameworks — principally the Budapest Convention, NIST SP 800-86, ISO/IEC 27037:2012, and the ACPO Principles — to identify the elements of a workable alternative. Part VII proposes the Forensic Authenticity Framework (FAF) and outlines the legislative and judicial steps necessary for its implementation. Part VIII concludes with the constitutional case for urgency.

II. THE TRIPARTITE LEGISLATIVE ARCHITECTURE

A. Bharatiya Sakshya Adhiniyam 2023: The Evidentiary Pillar

The BSA 2023, which came into force on 1 July 2024, repeals the Indian Evidence Act 1872 and introduces a modernised evidentiary framework responsive to the Supreme Court's accumulated digital evidence jurisprudence. In the domain of electronic records, the BSA retains the structural architecture of its predecessor while introducing refinements that partially address the interpretive controversies generated by two decades of Section 65B litigation.

Sections 61 to 65 of the BSA govern the admissibility of electronic records, preserving the distinction between primary and secondary electronic evidence within a more technologically neutral framework. Section 63[5] (the functional successor to Section 65B of the Indian Evidence Act) retains the certification mechanism as the primary gateway for the admissibility of electronic records produced by a computer. The certificate, issued by a responsible official with knowledge of the computer's operation, must attest to: (i) the regularity of the computer's use during the relevant period; (ii) the reliability of the information stored; and (iii) the accuracy of the reproduction. Responding to the Supreme Court's guidance

[5]BSA 2023, s 63 (the successor provision to s 65B of the Indian Evidence Act 1872).

in *Arjun Panditrao*[6], the BSA contemplates circumstances in which the court may, on application, direct the production of a certificate where the party relying on electronic evidence cannot independently procure it.

Sections 81A to 85C of the BSA[7] establish presumptions regarding electronic records, that digital signatures, electronic contracts, and records produced by automated banking systems are presumed genuine unless rebutted. These presumptions shift the evidentiary burden in breach cases, potentially allowing prosecution to rely on system logs and breach notification records as presumptively authentic documents.

However, the BSA 2023 contains a critical lacuna for data breach litigation: it does not address the admissibility of forensic reports generated during breach investigations, nor does it stipulate standards for the accreditation of forensic laboratories or the qualification of forensic experts as witnesses. The consequence is that the admissibility of forensic evidence in breach cases depends on the court's ad hoc assessment of the expert's credibility rather than on a structured statutory standard — a deficiency examined as the First Deficit in Part V.

B. Digital Personal Data Protection Act 2023: The Unintegrated Evidentiary Source

The DPDPA 2023 represents India's first comprehensive statutory response to the international data protection paradigm. For present purposes, its most significant contribution to the evidentiary landscape is the mandatory breach notification obligation imposed on Data Fiduciaries under Section 8(6)[8] of the Act, read with forthcoming Data Protection Board regulations.

Under this provision, a Data Fiduciary is required to notify the Data Protection Board and affected Data Principals of a personal data breach. The notification must contain specified particulars: the nature of the breach, the categories of data affected, the likely consequences, and the measures taken or proposed. These notifications, prepared under a statutory obligation that attracts penal consequences for inaccuracy and filed with a regulatory body, constitute a

[6]The proviso reflects the Supreme Court's direction in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 [60], which contemplated judicial direction for production of the certificate where the party cannot independently procure it.
[7]BSA 2023, ss 81A–85C.
[8]DPDPA 2023, s 8(6).

new and potentially significant category of documentary evidence in breach litigation.[9]

From an evidentiary perspective, the DPDPA breach notification record possesses characteristics that make it potentially more reliable than post-hoc forensic reconstruction: it is contemporaneous with the breach event; it is prepared under a statutory duty of accuracy; and it is filed with a regulatory authority, creating an official documentary record. Yet the DPDPA 2023 contains no provision addressing how breach notification records should be treated as evidence in criminal or civil proceedings under the IT Act or the BSA 2023. This statutory silence, termed the *DPDPA-BSA Interoperability Failure* in Part V — constitutes the second structural deficit in India's data breach evidentiary framework.

C. Information Technology Act 2000: The Penalization Framework

The IT Act 2000 remains the primary statutory source of criminal liability for data breach offences. Section 43 imposes civil liability for unauthorized access and data damage. Section 66 criminalizes computer-related offences, prescribing imprisonment of up to three years or a fine of up to five lakh rupees. Sections 66B, 66C, and 66D address the receipt of stolen computer resources, identity theft, and online fraud, respectively. Sections 72 and 72A impose penalties for breaches of confidentiality and unauthorised disclosure of information.[10]

Critically, Section 70B[11] designates CERT-In as the national agency for cybersecurity incident response and mandates breach reporting by designated entities. CERT-In's 2022 Directions[12] significantly expand these obligations, requiring covered entities to maintain system logs for 180 days and to report incidents within six hours of discovery. These CERT-In-mandated logs and incident reports constitute a distinct category of forensic documentary evidence in breach prosecutions, yet, like DPDPA breach notifications, they exist in a legislative space that the BSA 2023 has not been calibrated to receive, producing the interoperability failure diagnosed in Part V.

[9]DPDPA 2023, s 8(6); see also the Data Protection Board of India's forthcoming regulations on breach notification timelines, expected to prescribe a 72-hour notification period in alignment with global best practice.
[10]IT Act (n 3) ss 43, 66, 66B, 66C, 66D, 72, 72A.
[11]IT Act (n 3) s 70B.
[12]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 for Safe & Trusted Internet' (Ministry of Electronics and Information Technology, 28 April 2022) cls 3, 6.

III. THE FORENSIC-EVIDENTIARY INTERFACE: MECHANISMS, METHODOLOGIES, AND THE CERTIFICATION BOTTLENECK

A. Taxonomy of Digital Forensics in Breach Investigations

Digital forensics encompasses a family of investigative disciplines that share a common methodological commitment: the identification, preservation, acquisition, and analysis of digital material in a manner that maintains the evidential integrity of the data throughout the investigative process.[13] In data breach cases, four branches of digital forensics are most commonly engaged.

Computer Forensics involves the examination of storage media — hard drives, solid-state drives, and removable media — to recover, reconstruct, and analyse digital artifacts such as deleted files, system logs, and access timestamps. The forensic imaging methodology, which creates a bit-for-bit replica of storage media to preserve the original, is foundational to computer forensics and is governed internationally by ISO/IEC 27037:2012.[14]

Network Forensics involves the capture and analysis of network traffic data to reconstruct the timeline of unauthorized access, identify the ingress point, trace the exfiltration path, and attribute the breach to a source. Network forensics evidence is particularly complex from an evidentiary standpoint because it is inherently volatile — network traffic data dissipates without deliberate capture — and its reconstruction requires expertise in network protocol analysis that investigating police officers rarely possess.[15]

Mobile Forensics involves the extraction and analysis of data from smartphones, tablets, and IoT devices implicated in breach events, raising distinct challenges around device encryption, cloud backup systems, and the admissibility of data extracted from messaging applications under end-to-end encryption protocols.

Cloud Forensics, an emerging discipline, involves the recovery of evidence from third-

[13]Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd edn, Academic Press 2011) 7.
[14]International Organization for Standardization, ISO/IEC 27037:2012 Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (ISO 2012) cl 7.2.
[15]Casey (n 13) 389.

party cloud infrastructure located in foreign jurisdictions.[16] Cloud forensics raises profound jurisdictional questions regarding lawful access under the Budapest Convention's Article 32 and the mutual legal assistance treaty (MLAT) regime, dimensions that India's current legislative framework does not adequately address.

B. Chain of Custody: From Technical Protocol to Legal Doctrine

The chain of custody — the documented, unbroken record of every person who has handled a piece of evidence from collection through court presentation — is simultaneously a technical protocol and a legal doctrine of foundational importance in breach litigation.[17] At the technical level, chain of custody requires that each handover of digital evidence be documented with the date, time, identity of the transferor and transferee, and the condition of the evidence at transfer. At the legal level, a break in the chain of custody does not automatically render evidence inadmissible but creates a basis for challenging its integrity, a challenge that, in the context of digital evidence susceptible to undetected manipulation, carries particular weight.

The Supreme Court recognised the significance of the chain of custody in *Tomaso Bruno v State of Uttar Pradesh* (2015) 7 SCC 178, where it held that the reliability of digital evidence is contingent on proper procedural documentation of the custody sequence.[18] Under the BNSS 2023, Sections 94–99[19] prescribe search and seizure procedures for electronic devices. However, these provisions do not prescribe a specific chain of custody documentation format, leaving implementation to the discretion of investigating agencies, notably an absence that generates interpretive inconsistency across jurisdictions and forensic laboratories.

C. Section 65B Certification: Structure, Critique, and the Certification Bottleneck

The certification requirement (now in Section 63 of the BSA 2023) was intended to provide a technical guarantee of reliability by requiring a responsible official to certify the conditions of the computer's operation, the regularity of its use, and the accuracy of the reproduction. In practice, it has created what this paper terms the *Certification Bottleneck*: a procedural gatekeeping mechanism that courts have interpreted inconsistently, that prosecutors

[16]Stephen Mason (ed), Electronic Evidence (4th edn, Institute of Advanced Legal Studies 2017) ch 10.
[17]Bill Nelson, Amelia Phillips and Christopher Steuart, Guide to Computer Forensics and Investigations (5th edn, Cengage Learning 2014) 29.
[18]Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178 [24].
[19]Bharatiya Nagarik Suraksha Sanhita 2023 (No 45 of 2023) (BNSS 2023) ss 94–99.

frequently fail to satisfy, and that has resulted in the exclusion of otherwise reliable electronic evidence in breach cases.[20]

The certification mechanism presupposes a relatively simple evidentiary scenario: a record is produced on a known, regularly-used computer by an identifiable organization, and an official of that organization can certify its provenance. This model fits corporate financial records, email archives, and website content. It fits far less well the forensic artifacts generated in breach investigations: network flow data captured in real-time by forensic tools; memory images extracted from compromised servers; malware samples reverse-engineered by incident response analysts. In these cases, the "computer" is often the forensic investigator's workstation, the "responsible official" is a contracted forensic analyst, and the reliability of the output depends not on the regularity of computer use but on the scientific validity of the forensic methodology — a dimension that Section 63 BSA does not address.

IV. JUDICIAL TRAJECTORY: CHARTING INDIA'S DIGITAL EVIDENCE JURISPRUDENCE

A. The Pre-BSA Regime: From Navjyot Sandhu to Anvar PV

The Supreme Court's engagement with electronic evidence began in earnest in *State (NCT of Delhi) v Navjyot Sandhu* (2005) 11 SCC 600, a terrorism prosecution in which call records were admitted in evidence without strict compliance with Section 65B certification.[21] The Court, adopting a pragmatic approach, held that the strict rule of evidence must yield where the electronic record corroborates other evidence and its authenticity is not genuinely in dispute. This relaxed approach, whilst understandable in the context of a terrorism prosecution, generated a substantial body of lower court practice in which Section 65B certification was routinely overlooked, undermining the procedural integrity of digital evidence in a wider range of cybercrime proceedings.

The jurisprudential inconsistency generated by *Navjyot Sandhu* was addressed comprehensively in *Anvar PV v PK Basheer* (2014) 10 SCC 473, where a five-judge bench overruled the earlier decision and held that Section 65B certification is mandatory for the

[20]Ratanlal & Dhirajlal, The Law of Evidence (28th edn, LexisNexis 2023) 847–52.
[21]State (NCT of Delhi) v Navjyot Sandhu (2005) 11 SCC 600 [150]–[152].

admissibility of electronic records, admitting of no exception.[22] The Court reasoned that the legislature had specifically devised the certification mechanism as the exclusive mode of proving electronic records, and that the secondary evidence route under Section 65 of the Indian Evidence Act was not available as an alternative pathway. While *Anvar PV* resolved the doctrinal ambiguity at the macro-level, it did so at the cost of practical flexibility — a rigidity that created hardship for parties who could not obtain a certificate because the certifying official was unavailable, the computer had been disposed of, or the record predated the party's access to the system.

B. The Arjun Panditrao Watershed

In *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1, a five-judge Constitution Bench reaffirmed the mandatory nature of Section 65B certification while introducing an important qualification: where the certificate cannot be produced by the party relying on the electronic record because it is in the custody of the adverse party or a third party, the trial court may, under its inherent powers, direct its production.[23] The judgment has been widely received as a practical compromise between the absolutism of *Anvar PV* and the pragmatism of *Navjyot Sandhu*.

However, from the perspective of data breach litigation, *Arjun Panditrao* has significant limitations. The judicial direction remedy is available only where the certificate-issuing party is identifiable and within the court's jurisdiction, a condition rarely satisfied in transnational breach cases where forensic artefacts may have been generated by servers located in multiple foreign jurisdictions. More fundamentally, the judgment concerns itself exclusively with the certification mechanism and does not address the broader question of how courts should evaluate the scientific reliability of the forensic methodology used to generate the electronic record — the First Deficit diagnosed in Part V.

C. Post-2020 Developments and Remaining Ambiguities

The transition to the BSA 2023 has introduced additional uncertainties. Section 63 of the BSA expands the definition of "computer" to encompass server farms, cloud computing infrastructure, and IoT systems, but retains the certification mechanism as the primary

[22] Anvar PV v PK Basheer (2014) 10 SCC 473 [14], [22].
[23] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 [56], [66].

admissibility gateway. The question of whether *Arjun Panditrao's* interpretation applies with equal force to Section 63 BSA has not been judicially resolved, creating interpretive lacunae that are particularly acute during the transitional period.

The Supreme Court's guidance in *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801, affirming that Section 65B certification is not required where the original electronic device is produced before the court applies in a limited class of breach cases where the primary storage device is physically available. In the more common scenario, where evidence exists in fragmented form across network logs, memory dumps, and cloud repositories, *Shafhi Mohammad* provides no practical guidance. Similarly, *Sonu v State of Haryana* (2017) 8 SCC 570 observed that trial courts regularly demonstrate insufficient understanding of the technical dimensions of electronic evidence,[24] yet the judgment stops short of prescribing a remedial standard. The cumulative effect of these judicial developments is a framework that has resolved the gatekeeping question but left the substance of forensic reliability evaluation entirely to ad hoc judicial discretion.

V. THE AUTHENTICATION PARADOX: DIAGNOSING THE TRIPARTITE DEFICIT

A. The First Deficit: The Forensic Methodology Vacuum

The most fundamental structural deficit in India's data breach evidentiary framework is the absence of any statutory or judicially developed standard for evaluating the scientific reliability of forensic methodologies. This deficit — the *Forensic Methodology Vacuum* — means that the admissibility of forensic evidence in breach cases depends entirely on whether the formal procedural gateway of Section 63 BSA has been satisfied, without any inquiry into whether the forensic method employed to generate the evidence meets a threshold of scientific validity.

The contrast with United States federal evidence law is instructive. The *Daubert* standard[25] requires a trial judge to perform a gatekeeping function in assessing whether expert testimony is based on sufficient facts or data, is the product of reliable principles and methods,

[24]Sonu v State of Haryana (2017) 8 SCC 570 [12].
[25]Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993) 589–595 (Blackmun J), establishing the federal trial court's gatekeeping function in assessing the reliability of expert scientific testimony.

and has been reliably applied to the facts of the case. While the *Daubert* standard has its critics[26] (particularly for the burden it places on generalist judges to evaluate specialised scientific questions), it represents a recognition that procedural compliance alone cannot substitute for substantive reliability assessment. India's framework, in which Section 63 certification is both necessary and sufficient for admissibility (absent challenges to its procedural compliance), has no equivalent gatekeeping mechanism for forensic reliability.

The consequence of the Forensic Methodology Vacuum is acutely visible in cases involving malware forensics, where the chain of attribution depends on the scientific reliability of the reverse engineering methodology. Courts lack any structured framework for assessing whether the forensic analyst has employed peer-reviewed methodologies, whether the tools used have been scientifically validated, or whether the results have been independently verified. This gap creates a false negative risk (reliable forensic evidence is excluded for want of certification) and a false positive risk (unreliable forensic evidence is admitted because a certificate has been produced).

B. The Second Deficit: The DPDPA-BSA Interoperability Failure

The *DPDPA-BSA Interoperability Failure* operates at the intersection of substantive data protection law and evidentiary law. Under Section 8(6) of the DPDPA 2023, Data Fiduciary breach notifications to the Data Protection Board constitute the most contemporaneous and officially recorded documentary evidence of the occurrence, scope, and impact of a data breach. They are prepared under a statutory duty of accuracy, filed with a regulatory body, and preserved in an official register. Yet the DPDPA 2023 contains no provision addressing how breach notification records should be treated under the BSA 2023's evidentiary framework.[27]

Ought to breach notifications be treated as public documents under Section 74 of the BSA, admissible without further proof? Are they electronic records subject to Section 63 certification? Can they be relied upon as admissions against the Data Fiduciary in criminal proceedings under the IT Act? These questions remain entirely open. Their resolution through ad hoc judicial interpretation, rather than legislative design, is likely to generate the same

[26]Erica Beecher-Monas, Evaluating Scientific Evidence: An Interdisciplinary Framework for Intellectual Due Process (Cambridge University Press 2007) ch 2.
[27]CERT-In Directions (n 12) cl 3, requiring cyber incident reports to be filed within six hours of discovery, with system logs retained for 180 days.

fragmentation that characterised the Section 65B jurisprudence before *Anvar PV*. The CERT-In incident reporting obligation compounds this failure: logs filed under penal obligation with a statutory regulatory body within six hours of a breach[28] would appear to satisfy the hallmarks of presumptively authentic documentary evidence, yet the BSA does not address their admissibility in criminal proceedings.

C. The Third Deficit: Judicial Capacity and Interpretive Inconsistency

The third structural deficit is the interpretive inconsistency that results from adjudicating technically complex forensic evidence without specialised judicial capacity or principled standards. The Supreme Court has resolved the macro-level question of whether Section 65B certification is mandatory. The micro-level questions that arise in data breach litigation — how to evaluate conflicting forensic reports from prosecution and defence experts; how to assess the reliability of IP address attribution evidence in cases of VPN or Tor usage; how to treat timestamp evidence in systems configured for a different time zone — remain without principled resolution.

This interpretive inconsistency has concrete systemic consequences. As observed in *Sonu v State of Haryana*, trial courts regularly demonstrate insufficient understanding of the technical dimensions of electronic evidence, resulting in either the wholesale rejection of forensic evidence or its uncritical acceptance. The absence of a structured standard for forensic evidence assessment means that the quality of forensic evidence adjudication in breach cases depends, to an unacceptable degree, on the individual court's technical competence. This is not merely an efficiency concern: it is a rule of law concern, since identical forensic evidence may be admitted in one court and excluded in another on grounds that are not principled but adventitious.

VI. COMPARATIVE HORIZONS: INTERNATIONAL STANDARDS AND THEIR DOMESTIC RELEVANCE

A. The Budapest Convention: Mutual Assistance and Evidence Preservation

The Council of Europe's Convention on Cybercrime (Budapest Convention, ETS No 185), to which India is not yet a party but which functions as a normative benchmark,

[28] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 [56].

establishes a framework for both substantive cybercrime law harmonisation and procedural cooperation in evidence gathering. Articles 16 and 17 require State parties to provide for expedited preservation of stored computer data pending mutual legal assistance requests[29] — a direct legislative response to the evidentiary challenge of volatile digital evidence.

Articles 20 and 32 of the Budapest Convention provide respectively for real-time collection of traffic data and for a State party's access to publicly available stored computer data or, with consent, to stored data located in another State.[30] These provisions represent a sophisticated legislative response to the jurisdictional fragmentation that characterises cloud forensics — a domain in which India's current legislative framework is entirely silent. India's accession to the Second Additional Protocol[31], which significantly enhances the framework for cross-border disclosure of electronic evidence, remains pending, creating a gap in India's capacity to gather and receive digital evidence in transnational breach cases that is likely to deepen as breach actors increasingly exploit cross-jurisdictional cloud infrastructure.

B. NIST SP 800-86 and ISO/IEC 27037:2012: Technical Benchmarks

The National Institute of Standards and Technology's Special Publication 800-86[32] provides a four-phase forensic process framework — Collection, Examination, Analysis, and Reporting — that prescribes a structured methodology for ensuring evidentiary integrity at each stage. Critically, SP 800-86 emphasises the documentation of the forensic process, including the tools and techniques employed, as a precondition for the reliability of forensic findings, establishing a direct link between methodological documentation and evidentiary admissibility.

ISO/IEC 27037:2012[33] complements NIST SP 800-86 by providing internationally standardised guidelines for the identification, collection, acquisition, and preservation of digital evidence. Clause 7 of the standard specifies that digital evidence should be acquired using a validated, repeatable, and documented methodology; that the acquisition process should preserve the integrity of the original data through hash verification; and that the forensic

[29]Council of Europe, Convention on Cybercrime (Budapest Convention) (ETS No 185, opened for signature 23 November 2001, entered into force 1 July 2004) arts 16–17.
[30]Budapest Convention (n 30) arts 20, 32.
[31]Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No 224, opened for signature 12 May 2022).
[32]National Institute of Standards and Technology, SP 800-86: Guide to Integrating Forensic Techniques into Incident Response (NIST 2006).
[33]ISO/IEC 27037:2012 (n 14) cl 6.

examiner should be technically competent and capable of explaining the methodology to a court. These criteria — validity, repeatability, documentation, hash verification, and competence — provide the technical substrate for the First Tier of the Forensic Authenticity Framework proposed in Part VII.

C. The ACPO Principles: A Workable Doctrinal Model

The Association of Chief Police Officers' Good Practice Guide for Digital Evidence[34] articulates four foundational principles for the handling of digital evidence that have influenced forensic practice in Commonwealth jurisdictions and internationally. These are: (i) *Non-Alteration*: no action taken by law enforcement should change data that may subsequently be relied upon in court; (ii) *Competence*: persons accessing original data must be competent to do so and able to give evidence explaining their actions; (iii) *Audit Trail*: a record of all processes applied to digital evidence should be created and preserved, sufficient to permit an independent third party to achieve the same result; and (iv) *Accountability*: the person in charge of the investigation bears overall responsibility for adherence to these principles.

The ACPO Principles are significant for present purposes not because they should be adopted wholesale into Indian law but because they demonstrate that a principled, workable doctrinal standard for digital forensics can be articulated with sufficient precision to guide both practitioners and courts. The Forensic Authenticity Framework, proposed in Part VII, translates these principles into a three-tier judicial admissibility standard calibrated to the specific challenges of data breach litigation in India.

VII. THE FORENSIC AUTHENTICITY FRAMEWORK: A PROPOSED REFORM

A. Structure and Rationale

The Forensic Authenticity Framework (FAF) proposed in this paper is a three-tier doctrinal standard designed to provide courts with a structured, judicially administrable methodology for evaluating forensic evidence in data breach litigation. The FAF operates as a condition of admissibility — not a standard of proof — and its three tiers address respectively the three structural deficits diagnosed in Part V. It is premised on the recognition that the procedural compliance gateway of Section 63 BSA, while necessary, is insufficient to

[34]Association of Chief Police Officers (ACPO), Good Practice Guide for Digital Evidence (5th edn, 2012).

guarantee the reliability of forensic evidence, and that courts require a substantive standard for evaluating the scientific validity, procedural integrity, and contextual reliability of digital forensic evidence presented in breach cases.

B. Tier One — Technical Integrity Assessment

The first tier addresses the Forensic Methodology Vacuum. Under Tier One, a court must satisfy itself that the forensic evidence sought to be admitted was generated through a methodology that satisfies three criteria.

(i) Methodological Validity: The forensic methodology employed must be scientifically valid — capable of producing reliable results when correctly applied. This does not require peer review of the specific analysis but does require that the technique used (e.g., hash verification, forensic imaging, malware reverse engineering) is a recognised methodology in the forensic community, as evidenced by its endorsement in NIST SP 800-86, ISO/IEC 27037:2012, or a comparable internationally recognised standard.

(ii) Tool Validation: The forensic tools used in the analysis must have been validated — either by the tool developer, by an independent laboratory, or by formal testing programmes such as NIST's Computer Forensics Tool Testing programme.[35] This criterion ensures that the evidential output of forensic software tools has not been compromised by bugs, miscalibration, or design limitations that could affect the accuracy of the forensic findings.

(iii) Reproducibility: The forensic process must be documented in sufficient detail that an independent forensic examiner, applying the same methodology to the same data, could reproduce the results. This is the forensic equivalent of the ACPO Good Practice Guide's Principle 3, and it provides the practical test of methodological reliability that courts can apply without possessing specialist technical expertise themselves.

C. Tier Two — Procedural Compliance Verification

The second tier addresses the DPDPA-BSA Interoperability Failure. Under Tier Two, a court must assess whether the forensic evidence was gathered, preserved, and documented in

[35]NIST, Computer Forensics Tool Testing Program < https://csrc.nist.gov/projects/computer-forensics > accessed 1 February 2026.

compliance with the applicable procedural requirements.

(i) Chain of Custody Documentation: The evidence must be accompanied by a documented chain of custody establishing that it has not been altered between collection and presentation. This subsumes the existing requirements under the BNSS 2023.

(ii) Section 63 BSA Certification: Where the forensic evidence takes the form of an electronic record, a certificate under Section 63 BSA must be provided or its production must have been sought through the court's direction power confirmed in *Arjun Panditrao*.[36] Critically, the FAF proposes that DPDPA breach notification records and CERT-In incident reports should be deemed to satisfy this certification requirement by operation of a statutory presumption — they are filed under penal obligation with regulatory bodies and constitute prima facie evidence of the facts stated therein.

(iii) Jurisdictional Compliance: Where forensic evidence has been gathered from servers or cloud infrastructure located in foreign jurisdictions, the court must verify that the evidence was obtained through a lawful access mechanism — whether through an MLAT request, a Budapest Convention preservation request, or the consent of the relevant service provider. Evidence obtained in violation of the legal access framework of the source jurisdiction should be inadmissible, consistent with the principle of comity and the proportionality requirements embedded in the right to privacy under Article 21.

D. Tier Three — Contextual Reliability Evaluation

The third tier addresses judicial interpretive inconsistency by providing a structured framework for assessing the probative value of forensic evidence in the specific factual context of the breach. Under Tier Three, the court considers:

(i) Expert Qualification: Whether the forensic analyst is appropriately qualified by formal credentials, such as Certified Information Systems Security Professional (CISSP), Certified Forensic Computer Examiner (CFCE), or equivalent, and by relevant experience in the type of forensic analysis performed. Statutory recognition of accredited forensic

[36] Arjun Panditrao Khotkar (n 23) [56] – [66].

laboratories under Section 79A of the IT Act[37] should be leveraged: the FAF proposes that reports issued by Section 79A-designated laboratories carry a rebuttable presumption of expert competence.

(ii) Corroborating Evidence: Whether the forensic evidence is corroborated by independent sources — such as CERT-In incident reports, DPDPA breach notifications, server access logs, or testimony from system administrators — that provide a convergent picture of the breach event. Convergence of independent evidentiary sources is a recognised indicia of reliability that courts are well-positioned to assess.

(iii) Counter-Expert Assessment: Where the defence has produced a competing forensic report, the court must evaluate the competing methodologies against the Tier One criteria rather than simply preferring the prosecution's expert by reason of institutional affiliation. This is consistent with the broader constitutional requirement, recognised in *Selvi v State of Karnataka*[38] and elaborated in the context of forensic evidence in *Ram Singh v Col Ram Singh*[39], that the investigative and adjudicative process must be principled rather than outcome-determined.

E. Legislative Implementation and Constitutional Grounding

The FAF can be implemented through two mechanisms. The primary mechanism is legislative amendment to the BSA 2023 — specifically, the insertion of a new section following Section 63 providing: (a) a forensic report in a data breach case shall be admissible as evidence of its contents where the court is satisfied that the forensic methodology is scientifically valid and recognised, the tools used have been validated, and the forensic process has been documented to permit independent reproduction; (b) a breach notification filed with the Data Protection Board under Section 8(6) of the DPDPA 2023, or a cybersecurity incident report filed with CERT-In under Section 70B of the IT Act, shall be admissible as evidence of the

[37]IT Act (n 3) s 79A, which designates the Central Forensic Science Laboratory (CFSL) and other laboratories as 'Examiner of Electronic Evidence' for purposes of providing expert opinions under s 45A, inserted by the Information Technology (Amendment) Act 2008 (No 10 of 2009).
[38]Selvi v State of Karnataka (2010) 7 SCC 263 [263] – [265] (CBI, Patnaik J), recognising the constitutional dimension of forensic evidence gathering under Article 20(3) and Article 21, and requiring that investigative methods comply with procedural due process.
[39]Ram Singh v Col Ram Singh (1985) 3 SCC 611 [17] – [18], an early instance of judicial caution regarding scientific evidence and the requirement that courts assess the methodology underlying expert conclusions.

facts stated therein without further proof and shall be deemed to satisfy the certification requirement under Section 63(4) of the BSA.

The constitutional grounding of the FAF is found in *KS Puttaswamy v Union of India* (2017) 10 SCC 1.[40] In recognising the right to informational privacy as a fundamental right under Article 21, the Supreme Court necessarily implied the existence of an effective legal remedy for breaches of that right. A legal framework that cannot effectively prosecute data breaches because forensic evidence is inadmissible for want of an appropriate evidentiary standard, fails to provide the effective remedy that Article 21 demands. *Ritesh Sinha v State of Uttar Pradesh*[41] further confirms that the constitutional dimension of personal liberty constrains the conditions under which forensic evidence may be gathered and compelled, reinforcing the need for a principled, rights-respecting forensic authentication standard. The FAF, by providing courts with a structured and judicially administrable methodology, gives institutional content to this constitutional requirement.

VIII. CONCLUSION

This paper has diagnosed a structural Authentication Paradox at the heart of India's data breach evidentiary framework. The tripartite legislative architecture of the BSA 2023, the DPDPA 2023, and the IT Act 2000 simultaneously generates the need for digital forensic evidence and fails to provide a coherent methodology for its evaluation. Three structural deficits — the Forensic Methodology Vacuum, the DPDPA-BSA Interoperability Failure, and judicial interpretive inconsistency — collectively undermine the effectiveness of forensic evidence in breach litigation and, by extension, the enforceability of India's emerging data protection architecture.

The judicial trajectory from *Navjyot Sandhu* through *Anvar PV* to *Arjun Panditrao* demonstrates that India's courts are capable of doctrinal evolution in the domain of digital evidence. But that evolution has been reactive rather than structural, addressing the symptom of the Certification Bottleneck while leaving the underlying deficits intact. The Forensic

[40]KS Puttaswamy v Union of India (2017) 10 SCC 1 [325] – [326] (Chandrachud J). See also KS Puttaswamy v Union of India (2019) 1 SCC 1 [375] – [379], affirming informational privacy as a component of the constitutional right to life and personal liberty under Article 21.

[41]Ritesh Sinha v State of Uttar Pradesh (2019) 8 SCC 1 [24], where the Supreme Court drew upon the constitutional dimension of personal liberty to circumscribe the conditions under which biometric evidence may be compelled, a principle with structural analogues in the compelled production of forensic decryption keys.

Authenticity Framework proposed in this paper offers a proactive and constitutionally grounded solution. By incorporating the technical reliability standards of NIST SP 800-86 and ISO/IEC 27037:2012, the procedural safeguards of the ACPO Principles, and a structured judicial assessment methodology that addresses expert qualification, corroborating evidence, and counter-expert evaluation, the FAF provides a three-tier standard capable of legislative and judicial implementation.

The urgency of reform is not abstract. India's digital economy continues to expand, and with it the frequency, sophistication, and cross-jurisdictional character of data breach events. The right to informational privacy, recognised as fundamental in *Puttaswamy*, demands a legal architecture capable of holding perpetrators accountable through reliable forensic evidence. That architecture must be built — through deliberate legislative design and principled judicial reasoning — on the foundations of evidentiary reliability, forensic integrity, and judicial competence: the three pillars on which the Forensic Authenticity Framework rests.

BIBLIOGRAPHY

Primary Sources: Legislation

Bharatiya Sakshya Adhiniyam 2023 (No 46 of 2023).

Bharatiya Nagarik Suraksha Sanhita 2023 (No 45 of 2023).

Digital Personal Data Protection Act 2023 (No 22 of 2023).

Information Technology Act 2000 (No 21 of 2000).

Information Technology (Amendment) Act 2008 (No 10 of 2009).

Indian Evidence Act 1872 (repealed).

Primary Sources: Cases

Anvar PV v PK Basheer (2014) 10 SCC 473.

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993).

KS Puttaswamy v Union of India (2017) 10 SCC 1.

KS Puttaswamy v Union of India (2019) 1 SCC 1.

Ram Singh v Col Ram Singh (1985) 3 SCC 611.

Ritesh Sinha v State of Uttar Pradesh (2019) 8 SCC 1.

Selvi v State of Karnataka (2010) 7 SCC 263.

Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801.

Sonu v State of Haryana (2017) 8 SCC 570.

State (NCT of Delhi) v Navjyot Sandhu (2005) 11 SCC 600.

Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178.

Primary Sources: International Instruments

Council of Europe, Convention on Cybercrime (Budapest Convention) (ETS No 185, opened for signature 23 November 2001, entered into force 1 July 2004).

Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No 224, opened for signature 12 May 2022).

International Organization for Standardization, ISO/IEC 27037:2012 Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (ISO 2012).

Secondary Sources: Books

Association of Chief Police Officers (ACPO), Good Practice Guide for Digital Evidence (5th edn, 2012).

Beecher-Monas E, Evaluating Scientific Evidence: An Interdisciplinary Framework for Intellectual Due Process (Cambridge University Press 2007).

Casey E, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd edn, Academic Press 2011).

Mason S (ed), Electronic Evidence (4th edn, Institute of Advanced Legal Studies 2017).

Nelson B, Phillips A and Steuart C, Guide to Computer Forensics and Investigations (5th edn, Cengage Learning 2014).

Ratanlal & Dhirajlal, The Law of Evidence (28th edn, LexisNexis 2023).

Seth K, Computers, Internet and New Technology Laws (2nd edn, LexisNexis 2016).

Sharma V, Information Technology Law and Practice (5th edn, Universal Law 2019).

Secondary Sources: Reports and Guidelines

CERT-In, Annual Report 2023 (Ministry of Electronics and Information Technology 2024).

CERT-In, 'Directions under Sub-Section (6) of Section 70B of the Information Technology Act 2000' (Ministry of Electronics and Information Technology, 28 April 2022).

National Institute of Standards and Technology, SP 800-86: Guide to Integrating Forensic Techniques into Incident Response (NIST 2006).

NIST, Computer Forensics Tool Testing Program <https://csrc.nist.gov/projects/computer-forensics> accessed 1 March 2025.